Brazil Operational Technology Management

Last updated: 10/08/2026

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products or services is intended or should be inferred.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Please read the ServiceNow Website Terms of Use at www.servicenow.com/terms-of-use.html

Company Headquarters
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

servicenow

Table of Contents

Operational Technology **5**

Operational Technology Management licensing and subscriptions 8

Subscriptions for OTM 9

Install ITOM SU Licensing 9

View subscription statistics for OTM 10

Review OTM resource usage against allocated subscription units 10

Check CI count used for OTM subscriptions 11

View CIs consuming OTM subscription units 12

OTM SU Licensing References 13

OT Manager Foundation 19

ServiceNow Otto for OT Service Management 20

Operational Technology Setup 22

Explore 23

Configure 26

Use 27

Reference 31

Operational Technology Manager 32

Explore 33

Configure 39

Integrate 59

Use 133

Reference 204

Operational Technology Discovery 214

Operational Technology Native Discovery components 215

IT Discovery for Operational Technology (OT) Networks 370

Industrial Process Manager 375

Explore the Industrial Process Manager 376

Configure the Industrial Process Manager 378

Use 405

Reference 434

Operational Technology Vulnerability Response 442

Explore 443

Configure 445

Integrate 455

Use 483

Reference 490

Operational Technology Incident Management 494

Explore 494

Configure 499

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use 514
Reference 531
Operational Technology Change Management 533
Explore 534
Configure 537
Use 547
Reference 560
Operational Technology Knowledge Management 562
Explore 562
Configure 563
Use 571
Reference 578
Operational Technology Request Management 581
Explore 582
Configure 583
Use 586
Reference 587
Recommended Actions for OTSM 592
Explore 592
Configure 594
Use 595
AI Enhanced Recommended Actions for OTSM 595
Explore 596
Configure 597
Use 599
Employee Center for OT 599
Explore 600
Configure 601
Use 601
Industrial Workspace 602
Explore 603
Configure 626
Use 648
Domain separation and OT 669

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology

Use ServiceNow® for Operational Technology (OT) to help your organization streamline operations, boost productivity, and maximize your Operational Technology up-time on the production floor through digital workflows.

Operational Technology overview

Watch an overview about Operational Technology and the ServiceNow Operational Technology Management solution.

https://player.vimeo.com/video/1136253660?h=6cb04e4c1c&badge=0&autopause=0&player_id=0&app_id=58479

Benefits in Operational Technology, Core Operations, and empowering Factory Workers

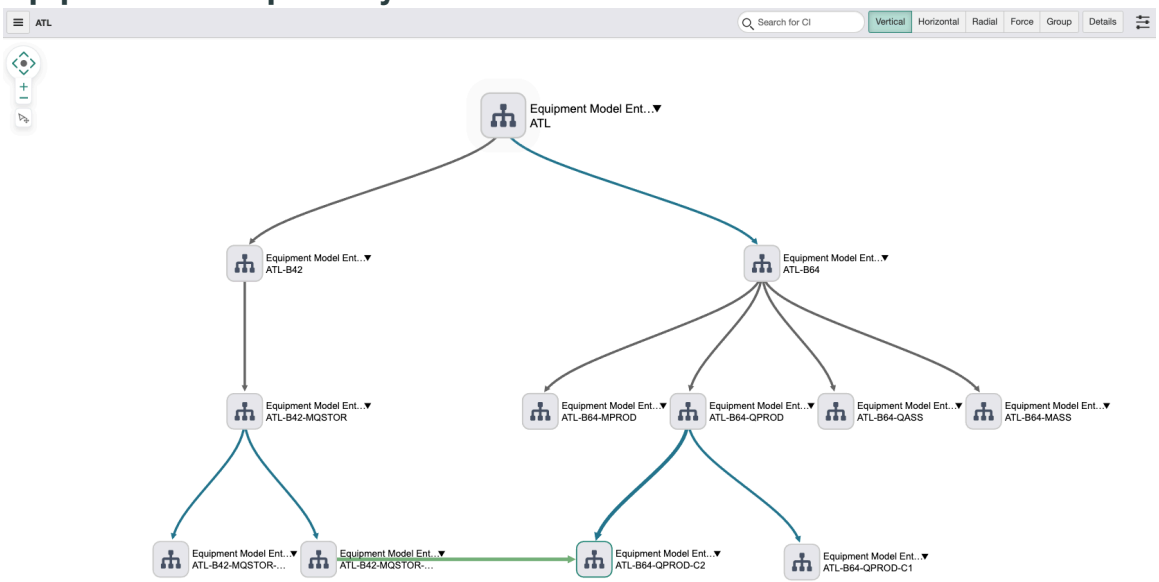


Maximize your uptime and build operational resilience with ServiceNow Operational Technology Management

Before industry Operational Technology, manufacturers depended on manual processes and legacy knowledge to maintain their environments. They found it challenging to get a complete view of their environments and to secure, monitor, and manage it all. With the ServiceNow Operational Technology Management solution, your industrial organization can now get a complete and contextual view of your operational technology systems. With this view, you can keep your systems secure, running, and connected to production processes and digital workflows. You can also enable your organization to assess, prioritize, and respond to events and threats.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Equipment model dependency view



By using a digital map, your organization can gain greater visibility of the industrial operations processes, systems, and relationships. With this map, you can manage and assess your potential production impacts easier and faster.

Note: The Operational Technology Management solution isn't supported on Now Mobile®.

Improve visibility 	Get a complete and contextual view of your Operational Technology systems, so that you can keep your systems secure and running.
Digital workflows 	Connect your Operational Technology systems to production processes and digital workflows.
Vulnerability management 	See everything in one place, so that you can assess, prioritize, and respond to events and threats.

Equip your workforce

Build low-code and no-code applications so that your employees can do collaborative monitoring, extended troubleshooting, problem-solving, and in-depth situational analysis.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See the solution brief for details.

Applications

- Operational Technology Manager

  Creates the foundational data and relationships that enable your organization to use the ServiceNow® OT solution.

- Operational Technology Discovery

  Amplifies the visibility of devices in your OT environment.

- Industrial Process Manager

  Creates the ISA-95 Equipment Model data foundation required for the ServiceNow® OT solution.

- Operational Technology Vulnerability Response

  Enables effective prioritization and remediation of OT device vulnerabilities at the site level.

- Operational Technology Incident Management

  Enables manufacturers to manage OT device incidents from open to closure.

- Operational Technology Change Management

  Enables your organization to implement changes to OT devices and production processes.

- Operational Technology Knowledge Management

  Helps you collect, organize, and share knowledge about your OT system, its devices, and the resolved incidents within your organization.

- Operational Technology Request Management

  Lets you request catalog items and fulfill them based on the defined flows.

- Recommended Actions for Operational Technology Service Management (OTSM)

  Allows you to set up and apply real-time actionable recommendations for speeding up the triaging process and resolving issues quickly across various records in the Industrial Workspace.

- AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

  Accesses external sources related to an OT incident, and contextualizes how the document is relevant to the incident.

- Employee Center for OT

  Central location where you can submit requests related to OT and industrial services.

- Industrial Workspace for Operational Technology

  User interface that provides you with the tools you need to manage your OT data.

- Service Management: IT Service Management

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security: Vulnerability Response
- Visibility: IT Operations Management

Get started

- Watch features demonstrated via DemoNow.
- For information on how to request and set up Operational Technology, see
  - Configuring the Operational Technology Manager
  - Configuring the OT Manager Foundation
  - Configure the Industrial Process Manager
  - Configuring Operational Technology Vulnerability Response
  - Configuring Operational Technology Incident Management
  - Configure ServiceNow Otto for Operational Technology (OT) Service Management
  - Configuring Operational Technology Change Management
  - Configuring Operational Technology Knowledge Management
  - Configuring Operational Technology Request Management
  - Configuring Recommended Actions for Operational Technology Service Management (OTSM)
  - Configure AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)
  - Configuring the Employee Center for OT
  - Configuring the Industrial Workspace
- For more information about how Operational Technology manages and uses Common Service Data Model tables, see Operational Technology and CSDM tables.
- For more information about the latest releases for Operational Technology, see ServiceNow Store - Operational Technology release notes.

Operational Technology Management licensing and subscriptions

ServiceNow® OTM licensing calculates and presents subscription usage based on subscription units. These units can include factors like the number of devices monitored or the subscription duration.

Operational Technology Management licensing and subscriptions overview

This enables organizations to ensure compliance, allocate resources effectively, and make informed decisions about scaling their OTM capabilities to safeguard their operational technology systems and adapt to changing security and operational needs. Use the OTM licensing module to access subscription-related details for the OTM products: ServiceNow OT Foundation, ServiceNow OT Visibility, and ServiceNow OT Vulnerability Response.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started

Explore OTM license	Install ITOM SU Licensing for OTM	Licensing References
		
Learn about subscription-related details	Update the latest version of plugin	Know about installed components like scheduled jobs and tables

Contact Support

Contact Customer Service and Support

Subscriptions for OTM

The ServiceNow platform employs OTM for license management in the manufacturing sector. OTM encompasses licenses found in IT Operations Management, along with licenses exclusive to the OTM domain.

Monitor OTM licenses in a manner similar to IT Operations Management licenses. Within the ServiceNow instance, you can identify OTM license types on the **ITOM Licensing Category MetaData** (**OTM License** > **Licenses by CI types**) page, where the **SKU Type** column displays a value of **otm**. By default, the license filter is set to **SKU Type** contains **otm**.

Install ITOM SU Licensing

Install or update the ServiceNow® ITOM SU Licensing [sn_itom_licensing] to ensure you use the latest licensing functionality. The application includes demo data and installs related ServiceNow® Store applications and plugins if they are not already installed.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- Review the ITOM SU Licensing application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.

Role required: admin

About this task

Prior to Q1 2022, the original licensing mechanism was delivered as part of the family releases. Since then the licensing mechanism is delivered using ServiceNow® ITOM SU Licensing on ServiceNow Store. The system automatically installs ServiceNow® ITOM SU Licensing. You receive notifications when updates for this application are available on ServiceNow Store.

The following items are installed with ITOM SU Licensing:

- Scheduled jobs
- Tables

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information, see Components installed with ITOM SU Licensing for OTM.

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the application (sn_itom_licensing) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find the application, you might have to request it from the ServiceNow Store.

   In the list next to the **Update** button, the versions that are available to you are displayed.
3. Select a version from the list and select **Update**.

   In the Install dialog that is displayed, any dependencies that are installed along with your application are listed.
4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. **Optional:** If demo data is available and you want to install it, select the **Load demo data** check box.
   Demo data are the sample records that describe application features for common use cases. Load the demo data when you first install the application on a development or test instance.
6. Select **Update**.

View subscription statistics for OTM

View the count of OTM application subscriptions purchased and consumed by your organization, offering valuable insights for resource management and operational technology optimization.

Before you begin

- Ensure your organization has active OTM subscriptions.
- Ensure that you installed the latest available version of the ITOM SU Licensing from ServiceNow Store.

Role required: sn_itom_license.reader

About this task

Evaluate the allocation of configuration items (CIs) and their allocation levels to assess the OTM subscription utilization of your organization and to prepare for future subscription requirements.

Procedure

1. To view subscription information for OTM subscriptions purchased a la carte, navigate to **OTM License** > **License Summary**.
2. Review the details presented on the form, as outlined in the Subscriptions form for the OTM products.

Review OTM resource usage against allocated subscription units

Review and analyze resource statistics that OTM products can manage and compare this information to the average allocation of subscription units.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Explore detailed licensing data trends of OTM using the OTM Licensing dashboard. Observe daily CI counts or view the averages for the last 90 daily counts. This feature provides domain-specific information and specific CI listings for each daily count, enabling you to effectively monitor and analyze resource usage over time.

Note: CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days.

Procedure

1. Navigate to **All** > **OTM License** > **OTM Licensing Dashboard**.
2. Select the relevant tab to display the dashboard for the OTM product.
3. Point to a bar to view the number of OT devices in each category.
4. Select the bar to view a list of the type of OT devices.
5. Review the dashboard described in OTM Licensing dashboard.

Check CI count used for OTM subscriptions

View the daily counts or the averages for the most recent 90 days of CI data. ServiceNow OT Foundation, ServiceNow OT Visibility and ServiceNow OT Vulnerability and Response offer insights into the licensed resources that OTM applications support. Resources that OTM applications discover, monitor, and provision are configuration items (CIs) stored in the CMDB. The OTM licensing module combines this CI information with the information on subscriptions your organization purchased to produce statistics on subscription use by OTM applications.

Before you begin

- Ensure your organization has active OTM subscriptions.
- Ensure that you installed the latest available version of the ITOM SU Licensing from ServiceNow Store.

Role required: sn_itom_license.reader

About this task

ServiceNow incurs charges for the usage of ServiceNow OT Foundation, ServiceNow OT Visibility and ServiceNow OT Vulnerability and Response. To gain a deeper understanding of the products and features included in OTM subscriptions, see Subscriptions for OTM.

The procedure for gathering and consolidating data for licensing purposes involves the following series of actions:

1. The OTM licensing system calculates the daily count of configuration items (CIs) managed by each OTM product, subsequently categorizing these CI counts into distinct licensable CI categories.
2. In some cases, identical configuration items (CIs) can be managed by various features within the same OTM products. In such cases, adjustments are made to eliminate any duplications in the CI count.
3. In cases where IT configuration items (IT CIs) are categorized as OT configuration items, the CIs are counted only once - under OTM licensing and not under ITOM licensing.
4. The licensing module consolidates CI counts from OTM applications to calculate the average of the daily CI count for the last 90 days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days ago.

5. The licensing module matches the daily average CI counts for OTM applications with the licensing details provided in the customer contract to generate license-related statistics.

Consequently, you can view the statistics on how your organization utilizes the purchased subscription units.

View information on CI count and subscriptions purchased for each OTM application separately (a la carte):

- **Total Count**: The average of the CI counts collected over 90 days, categorized by CI types, for each individual OTM application.

  Note: CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days ago.

- **Subscription Unit Ratio**: Ratios determine how many CIs of a particular CI category necessitate a subscription. The licensing module retrieves this ratio information from customer contracts.
- **Total Subscription Units Consumed**: The quantity of subscriptions used by your organization for each CI category within each OTM application. This calculation is performed by applying the subscription units ratio to the count of CIs within each respective CI category.
- **Total Subscription Units Consumed**: The total subscription units consumed by all OTM applications combined.

You can access OTM Subscription Unit (SU) consumption categorized by domain. This data can be useful for allocating consumption and expenses to different organizations.

Procedure

1. Navigate to **OTM License** > **License Report**.
2. **Optional:** View the average of daily CI counts for the last 90 days.
3. **Optional:** To view the daily CI counts, modify the filter to set **Aggregated** to **false**.

   (Optional) If needed, you can modify the view by sorting the columns. The **Created** column displays the timestamp indicating when the CI information was most recently updated.

View CIs consuming OTM subscription units

Generate a list of currently countable CIs for each of the OTM applications: ServiceNow® OT Foundation, ServiceNow® OT Visibility and ServiceNow® OT Vulnerability and Response.

Before you begin

- Ensure your organization has active OTM subscriptions.
- Ensure that you installed the latest available version of the ITOM SU Licensing from ServiceNow Store.

Role required: sn_itom_license.reader

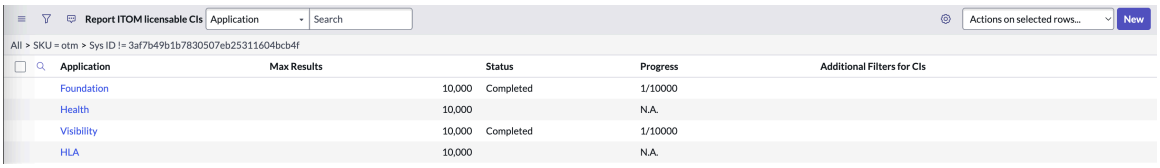
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The CI list generated is strongly correlated to the most recent daily count of CIs. However, the number of CIs on the generated list may display slight discrepancies compared to the latest daily count. This can occur if any changes have been made since the last daily count.

Procedure

1. Navigate to **All** > **OTM License** > **Report OTM Licensable CIs**.
   The **Report ITOM Licensable CIs** page appears.
2. Select the application for which you want to see licensed CIs.
   - Foundation
   - Visibility
   - HLA
   - Health



3. To create a report for the selected applications, select **Populate licensable CIs**.
4. To accept the confirmation message and generate the report, select **Yes**.

   The new report replaces the data in the previously generated report. You can cancel the report by selecting the application and then opting for the **Cancel Job** option.
5. Wait for a few minutes and then refresh the page.
   The application status is displayed as **Completed** once the report has finished processing.
6. Select the application and then select **Show licensable CIs**.

   The ITOM Licensable CIs page for OTM SKU displays the list of CIs with an OTM license.

OTM SU Licensing References

Use reference topics to gain valuable insights on the components installed with OTM licensing, subscription forms for OTM products, and an overview of the OTM licensing dashboard. Navigate the subtopics to access specific guidance and references on each of these critical aspects, helping you effectively manage your OTM subscriptions and licensing requirements.

Components installed with ITOM SU Licensing for OTM

Several types of components are installed with activation of the OTM SU Licensing plugin, including scheduled jobs and tables.

Scheduled jobs installed

Scheduled job	Description
ITOM Exclusion Tables Update Store	Updates the exclusion list.
ITOM Licensing Aggregator Store	Calculates the average of daily CI counts for the last 90 days.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Scheduled job	Description
ITOMHealthCIReporterWithOTOMCountOTOMStore	Compiles the list of licensable CIs for OTM Health.
ITOM Health Licensing Usage Count Store	Calculates the daily CI count for OTM Health.
OTOM Licensing Visibility CI Listing Store	Compiles the list of licensable CIs for OTM Visibility.
OTM Foundation Licensing CI Listing Store	Compiles the list of licensable CIs for OTM Foundation.
OTM Foundation Licensing Usage Count Store	Calculates the daily licensable CI counts for OT Foundation.

Tables installed

Table	Description
ITOM LU Discovery Source Mapping [itom_lu_discovery_source_mapping]	Contains the list of licensable discovery source for each category.
ITOM LU Governance App Mapping [itom_lu_governance_app_mapping]	List of records that contain the mapping of governance applications to their respective licensable CIs.
ITOM LU Governance CIs [itom_lu_governance_ci]	Contains the list of CIs counted under the Governance license.
ITOM License Exclusion Metadata [itom_license_exclusion_metadata]	Contains the list of exclusion rules applicable to different license.
License Exclusions [license_exclusion_list]	Contains the list of CIs that need to be excluded from the license count based on the exclusion rule.
Visibility LU Temporary [visibility_lu_temp]	Contains the list of CIs counted under the Discovery license.
ITOM Licensing Category MetaData [itom_lu_category_metadata]	Contains licensing metadata.
ITOM Licensing Discovery Sources [itom_lu_discovery_sources]	Contains the categories for all discovery sources.

Subscriptions form for the OTM products

Learn about the essential fields and indicators found on the Subscriptions form for our products, enabling streamlined subscription management and clarity in your OTM product usage.

View the following subscription statistics for items purchased individually (a la carte):

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name

The name of the OTM application.

Purchased

The number of purchased subscriptions per application.

Capacity Definition ID

The ID used for retrieving daily consumption data of subscription units from an application.

Start date/End date

The time duration during which this subscription remains active.

Subscriptions a la carte

The licensing module calculates and displays subscription consumption as follows:

Subscriptions a la carte

The Subscriptions window displays the information for purchased and allocated subscriptions for OTM applications.

OTM Licensing dashboard

Use the OTM Licensing dashboard to assess resource consumption and status in relation to your acquired subscriptions. The dashboard provides dedicated reports for each OTM application, providing visual representations of daily usage counts and the average utilization of subscription units over a 90-day period. The OTM Licensing dashboard is an integral component of ITOM Licensing application version 4.0, accessible at ServiceNow Store.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Required ServiceNow AI Platform roles

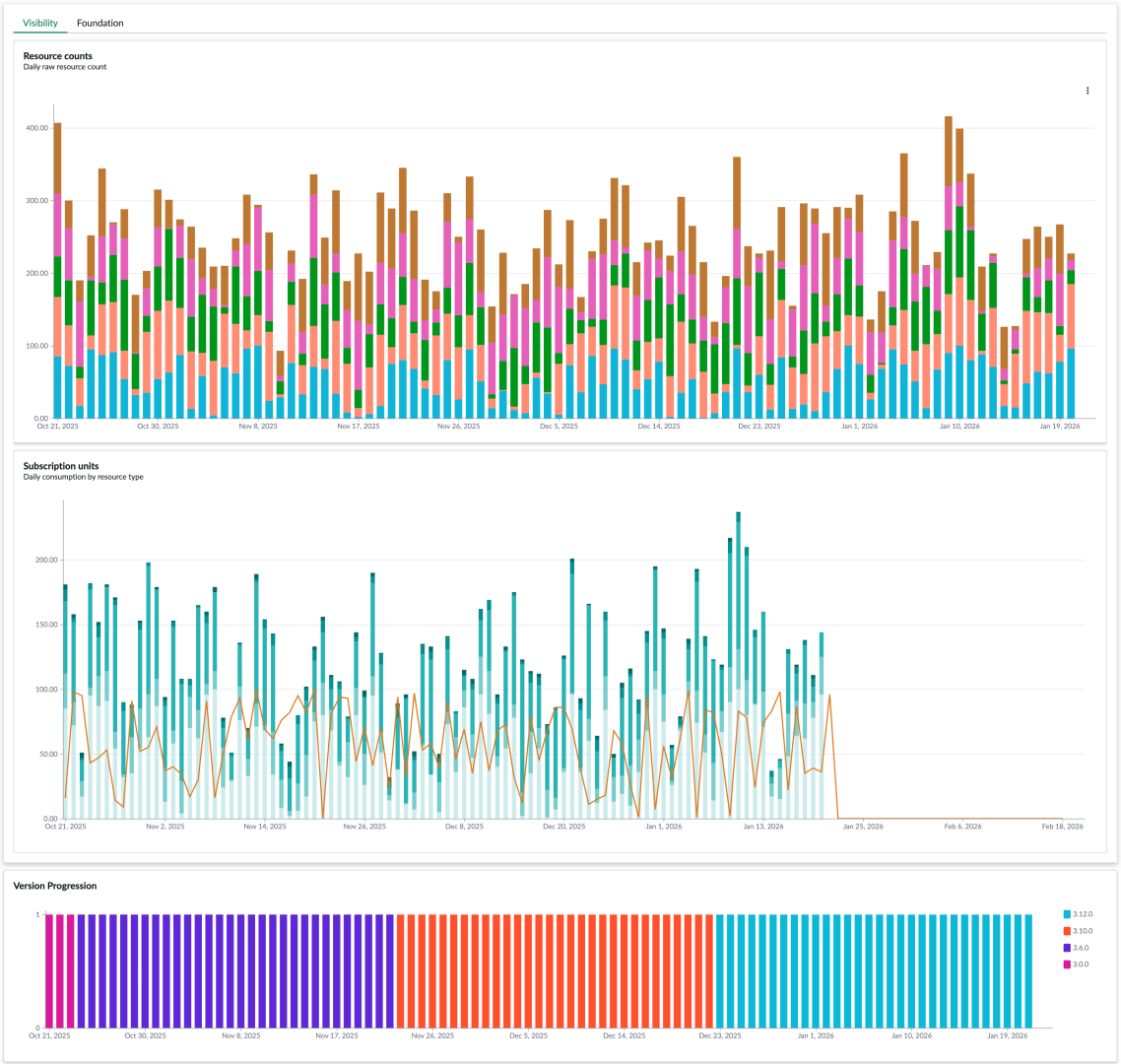
admin

Access the Assessment dashboard

To open the dashboard for OTM, navigate to **All** > **OTM License** > **OTM Licensing Dashboard**.

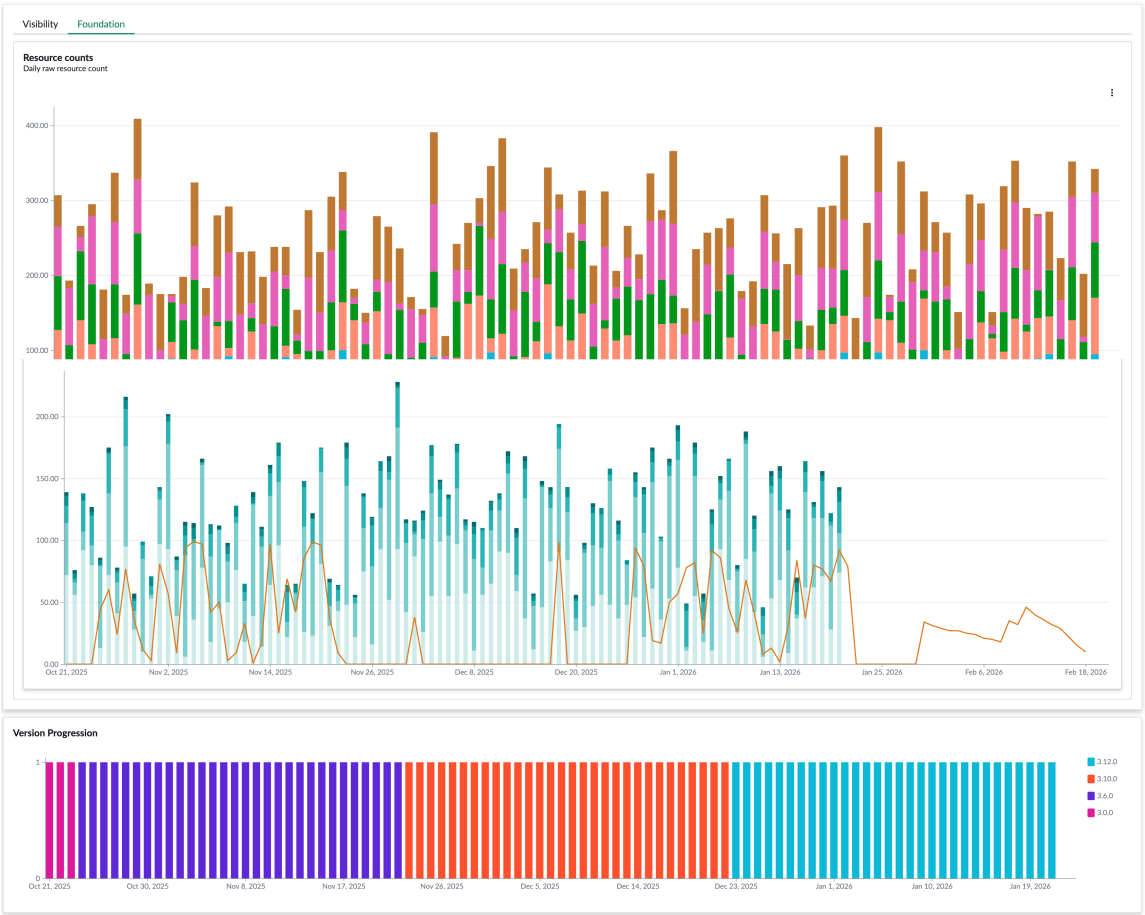
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OTM Licensing dashboard - Visibility



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OTM Licensing dashboard - Foundation



Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

User	Dashboard use
admin	Validate the resource usage for different OTM products. Report the cases where the organization exceeded the number of purchased subscription units for specific resources.

Note: ServiceNow applications refer to devices and applications that comprise an application service as configuration items (CIs).

Data visualization

The dashboard includes the following visualization:

Title	Source table	Description
OTM Visibility Usage and OTM Foundation Usage	ITOM Licensing CI Counts [itom_lu_ci_counts] and	The first area displays the daily raw resource

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Title	Source table	Description
	UsageAnalytics Counts for Tables [usageanalytics_count]	counts, which means all the detected resources before deduplication, normalization, and reconciliation required to sort them into specific CIs. **Note:** CIs managed by SG-OT Excel are counted and listed for license consumption with last_scan dates more recent than, equal to, and older than 90 days ago. Hover over the bars to see the table of resource types. Each type is shown with an absolute number of resources and a share it takes among others. The second area displays bars that represent Subscription units counts for different licensable categories for the last 120 days per OT application. The dashboard also displays the brown line that represents the UsageAnalytics counts for table. This count is based on average consumption of subscription units for the last 90 days. A SU ratio is used where one server, three PaaS resources, three containers, or one unresolved monitored object equal 1 SU. Hover over the vertical bar in the Subscription units area for the desired day to open the Available CIs list. The table shows each CI category included in the daily CI count, along with an absolute number of resources and a share it takes among others. The third area shows which version of the OTM Licensing is used on the instance every day. It helps explaining spikes

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Title	Source table	Description
		in count every time the new version is installed.

Operational Technology (OT) Manager Foundation

Use the Operational Technology (OT) Manager Foundation to help streamline processes in the Industrial Workspace related to your OT device data.

Get started

Note: Depending on your license, you will have access to certain application features, generative AI skills, agentic workflows, and AI agents. For more information, see ServiceNow product tiers.

Get started with AI

Starting with the Australia release, Now Assist for Operational Technology Manager (OTM) is being prepared for future deprecation. It will be hidden and no longer installed on new instances but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support Knowledge Base.

The ServiceNow AI Platform now brings you a new AI experience with three licensing tiers available:

- Foundation: AI basics to deliver insights
- Advanced: AI to boost productivity across relevant use cases
- Prime: Act autonomously with all AI assets, and create your own

For more information, see ServiceNow product tiers.

For more information about AI capabilities in Operational Technology Manager, see OT Manager Foundation.

For information about AI assets that are available on the ServiceNow AI Platform, see the following topics:

- Generative AI skills
- Agentic workflows

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important:

- Not all model providers are available for customers with in-country SKUs, and some AI products/features are currently unavailable for in-country customers. For more information, see the KB1584492 article in the Now Support Knowledge Base. Be sure to check for model provider availability updates in future releases.
- Some AI products/features are currently unavailable for customers in the FedRAMP, NSC DOD IL5, or Australia IRAP-Protected data centers, self-hosted customers, or in other restricted environments. For more information, see the KB0743854 article in the Now Support Knowledge Base. Be sure to check for availability updates in future releases.
- Some AI products/features are currently available only for customers in some regions. Be sure to check for availability updates in future releases.
- Some AI products and skills are not available in Regulated Markets. For more information, see KB2593939: Regulated Markets AI Products/Skills Not Available. Be sure to check for availability updates in future releases.

AI limitations

This application uses artificial intelligence (AI) and machine learning, which are rapidly evolving fields of study that generate predictions based on patterns in data. As a result, this application may not always produce accurate, complete, or appropriate information. Furthermore, there is no guarantee that this application has been fully trained or tested for your use case. To mitigate these issues, it is your responsibility to test and evaluate your use of this application for accuracy, harm, and appropriateness for your use case, employ human oversight of output, and refrain from relying solely on AI-generated outputs for decision-making purposes. This is especially important if you choose to deploy this application in areas with consequential impacts such as healthcare, finance, legal, employment, security, or infrastructure. You agree to abide by ServiceNow's AI Acceptable Use Policy, which may be updated by ServiceNow.

Data processing

This application requires data to be transferred from ServiceNow customers' individual instances to a centralized ServiceNow environment, which may be located in a different data center region from the one where your instance is, and potentially to a third-party cloud provider, such as Microsoft Azure. This data is handled per ServiceNow's internal policies and procedures, including our policies available through our CORE Compliance Portal.

Data collection

ServiceNow collects and uses the inputs, outputs, and edits to outputs of this application to develop and improve ServiceNow technologies including ServiceNow models and AI products. Customers can opt out of future data collection at any time, as described in the AI Opt-Out page.

ServiceNow Otto for Operational Technology (OT) Service Management

Use the ServiceNow Otto for Operational Technology (OT) Service Management application to summarize the Operational Technology (OT) incident information and generate incident resolution notes. You can enable your users to understand the context so that they can implement quicker resolutions.

Get started

Note: Depending on your license, you will have access to certain application features, generative AI skills, agentic workflows, and AI agents. For more information, see ServiceNow product tiers.

Get started with AI

Starting with the Australia release, Now Assist for Operational Technology Service Management (OTSM) is being prepared for future deprecation. It will be hidden and no longer installed on new instances but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support Knowledge Base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The ServiceNow AI Platform now brings you a new AI experience with three licensing tiers available:

- Foundation: AI basics to deliver insights
- Advanced: AI to boost productivity across relevant use cases
- Prime: Act autonomously with all AI assets, and create your own

For more information, see ServiceNow product tiers.

For more information about AI capabilities in Operational Technology Service Management, see ServiceNow Otto for OTSM.

For information about AI assets that are available on the ServiceNow AI Platform, see the following topics:

- Generative AI skills
- Agentic workflows

Important:

- Not all model providers are available for customers with in-country SKUs, and some AI products/features are currently unavailable for in-country customers. For more information, see the KB1584492 article in the Now Support Knowledge Base. Be sure to check for model provider availability updates in future releases.
- Some AI products/features are currently unavailable for customers in the FedRAMP, NSC DOD IL5, or Australia IRAP-Protected data centers, self-hosted customers, or in other restricted environments. For more information, see the KB0743854 article in the Now Support Knowledge Base. Be sure to check for availability updates in future releases.
- Some AI products/features are currently available only for customers in some regions. Be sure to check for availability updates in future releases.
- Some AI products and skills are not available in Regulated Markets. For more information, see KB2593939: Regulated Markets AI Products/Skills Not Available. Be sure to check for availability updates in future releases.

AI limitations

This application uses artificial intelligence (AI) and machine learning, which are rapidly evolving fields of study that generate predictions based on patterns in data. As a result, this application may not always produce accurate, complete, or appropriate information. Furthermore, there is no guarantee that this application has been fully trained or tested for your use case. To mitigate these issues, it is your responsibility to test and evaluate your use of this application for accuracy, harm, and appropriateness for your use case, employ human oversight of output, and refrain from relying solely on AI-generated outputs for decision-making purposes. This is especially important if you choose to deploy this application in areas with consequential impacts such as healthcare, finance, legal, employment, security, or infrastructure. You agree to abide by ServiceNow's AI Acceptable Use Policy, which may be updated by ServiceNow.

Data processing

This application requires data to be transferred from ServiceNow customers' individual instances to a centralized ServiceNow environment, which may be located in a different data center region from the one where your instance is, and potentially to a third-party cloud provider, such as Microsoft Azure. This data is handled per ServiceNow's internal policies and procedures, including our policies available through our CORE Compliance Portal.

Data collection

ServiceNow collects and uses the inputs, outputs, and edits to outputs of this application to develop and improve ServiceNow technologies including ServiceNow models and AI products. Customers can opt out of future data collection at any time, as described in the AI Opt-Out page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Setup

You can complete Operational Technology (OT) configuration items by navigating through the Admin Home and Product Hub, which use the ServiceNow Otto for Setup framework.

Get started

Explore  Learn more about how to use the Admin Home, Product Hub, and Configuration Console to complete Operational Technology configuration items	Configure  Access the Operational Technology card, Product Hub, and Configuration Console available from the Admin Home
Use  Complete the Operational Technology configuration items	Reference  Get details about related information

Helpful resources

Some ServiceNow resources that can provide you with helpful information are:

ServiceNow Community

ServiceNow Community

Developer

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow University

Best Practices

Best Practices

Partner

https://www.servicenow.com/partners.html

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ServiceNow

http://servicenow.com

ServiceNow Store

http://servicenow.com

Support

- https://support.servicenow.com/now
- Known Error Portal

Explore the Operational Technology Setup

Find out more about how the Admin Home, Product Hub, and Configuration Console from the ServiceNow Otto for Setup framework is used to access and complete Operational Technology (OT) configuration items.

ServiceNow Otto for Setup in Operational Technology

For Operational Technology (OT), ServiceNow Otto for Setup consolidates the setup processes for OT onto a single page, giving administrators a unified view of their configuration state.

Admin use case for ServiceNow Otto for Setup

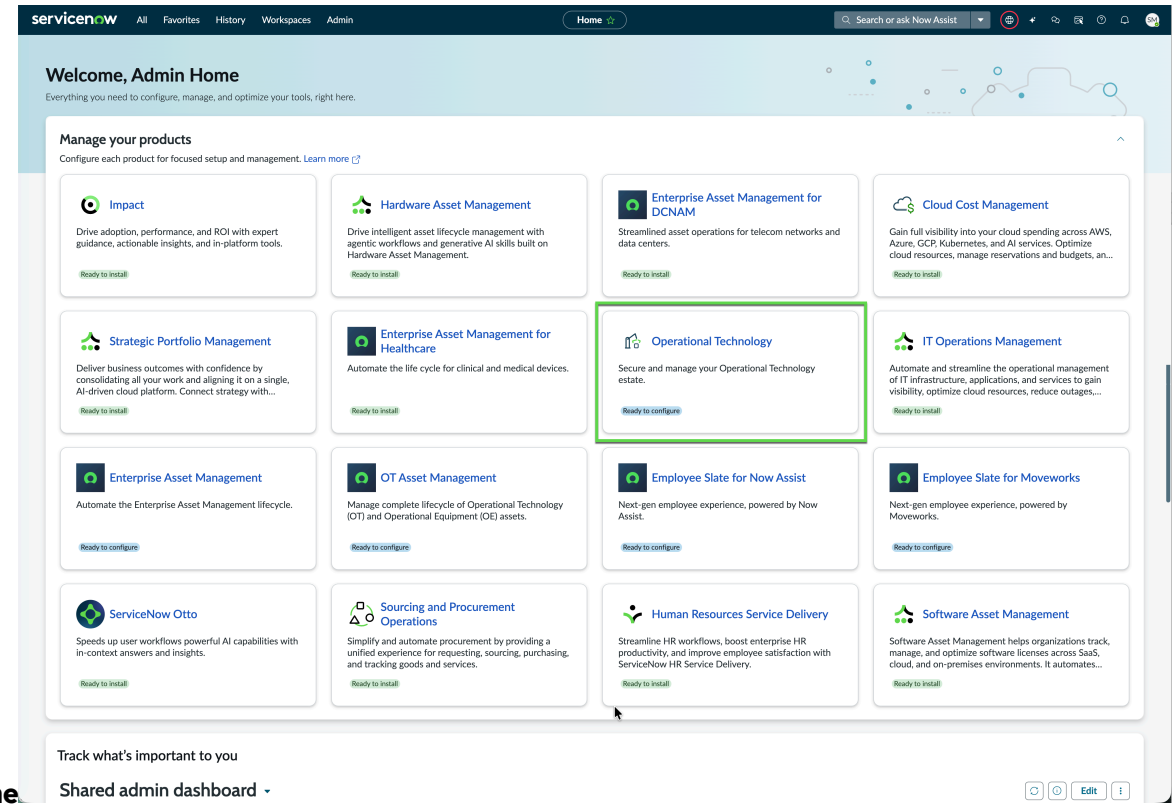
Configuring users, groups, and roles for your organization traditionally meant navigating between multiple pages to complete your administrative tasks. With ServiceNow Otto for Setup, administrators can create users, create user groups, and assign roles in a consolidated configuration console.

By opening the **Operational Technology** card on the Admin Home, administrators can access the Operational Technology Product Hub and Configuration Console to:

- Install the necessary OT applications
- Configure users, groups, and role assignments for OT

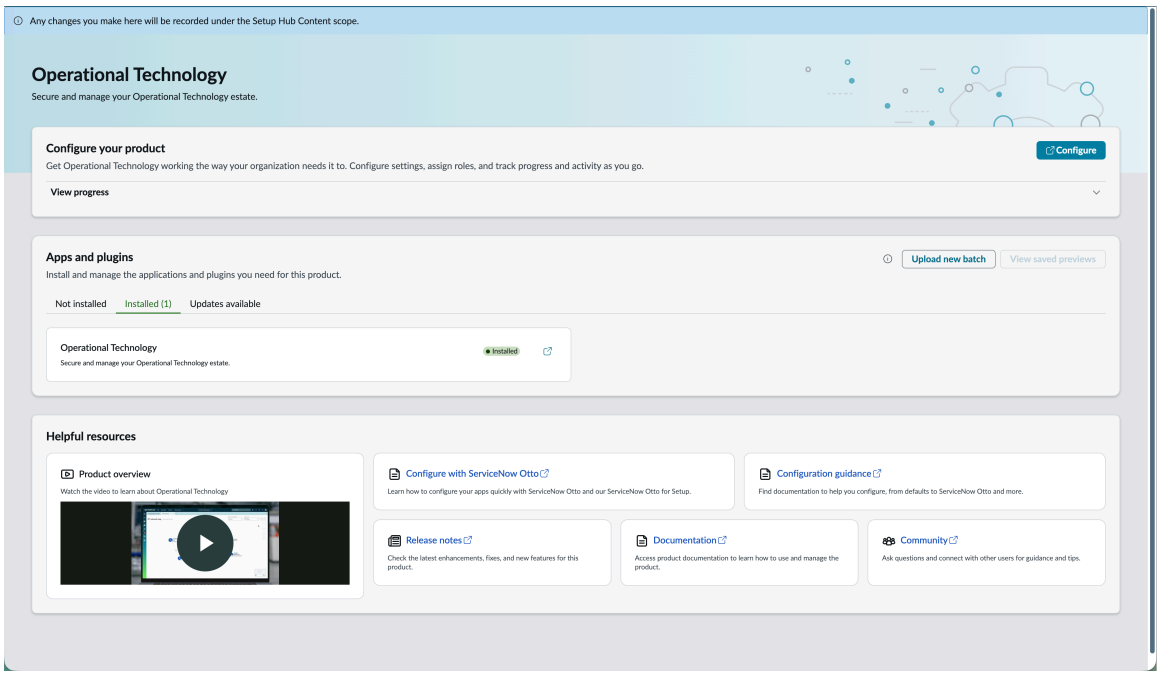
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Admin



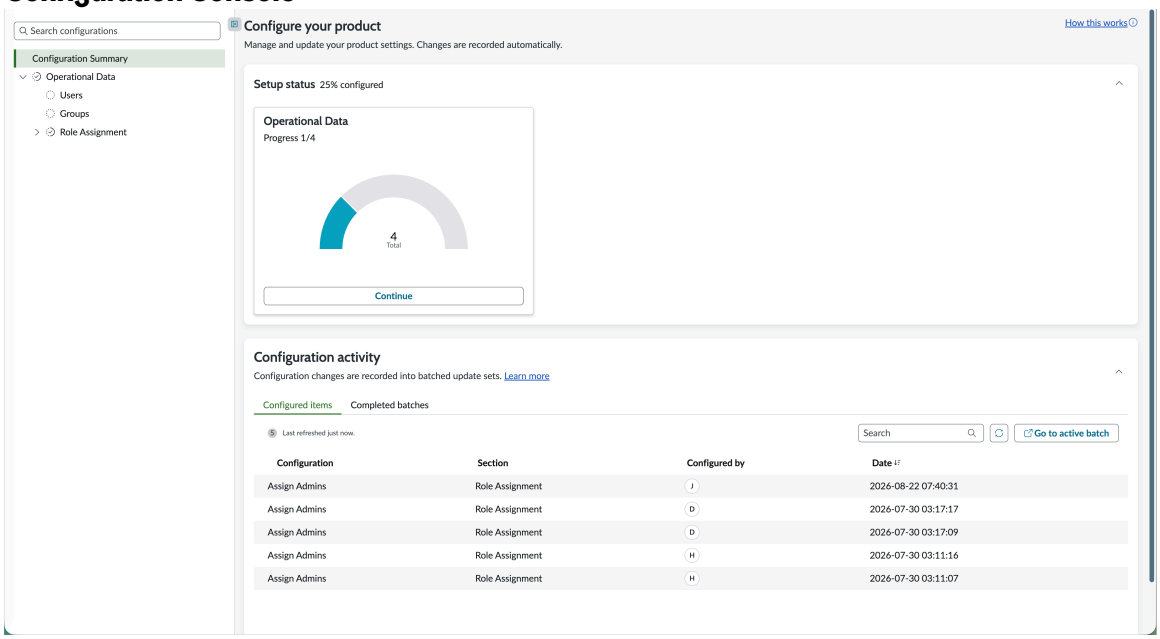
Home

Product Hub



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration Console



User permissions

User	Permissions
Administrator	Can use ServiceNow Otto for Setup to configure OT users, groups, and role assignments. Administrators can access the Admin Home, Operational Technology Product Hub, and Operational Technology Configuration Console.

OT workflow

The OT workflow for ServiceNow Otto for Setup moves through organized configuration items to complete.

1. Add OT users to your system, edit existing users, and assign multiple users to an OT group.
2. Add an OT group to organize users and assign roles per group.
3. Assign OT roles to a user or group.
4. Assign OT admin roles to admin users that manage configuration and operational control.

Benefits

ServiceNow Otto for Setup - OT benefits

Benefit	Feature	Users
Access and complete all OT configuration items in one place.	Operational Technology Setup configuration items	Administrator

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ServiceNow Otto for Setup - OT benefits (continued)

Benefit	Feature	Users
Reach the Configuration Console from the same Admin Home page that hosts other product configuration entry points.	Operational Technology card on the Admin Home page	Administrator

What to explore next

To learn more about accessing and using ServiceNow Otto for Setup for OT configuration, see:

- Access ServiceNow Otto for Setup (OT)
- Operational Technology Setup configuration items
- Add OT users
- Add an OT assignment group
- Assign OT roles
- Assign OT admin roles

Configure Operational Technology Setup

Verify you have access to the pages needed to complete the Operational Technology (OT) configuration items.

Access ServiceNow Otto for Setup (OT)

Use the Admin Home to access the Operational Technology (OT) card, and start setting up your organization's OT environment.

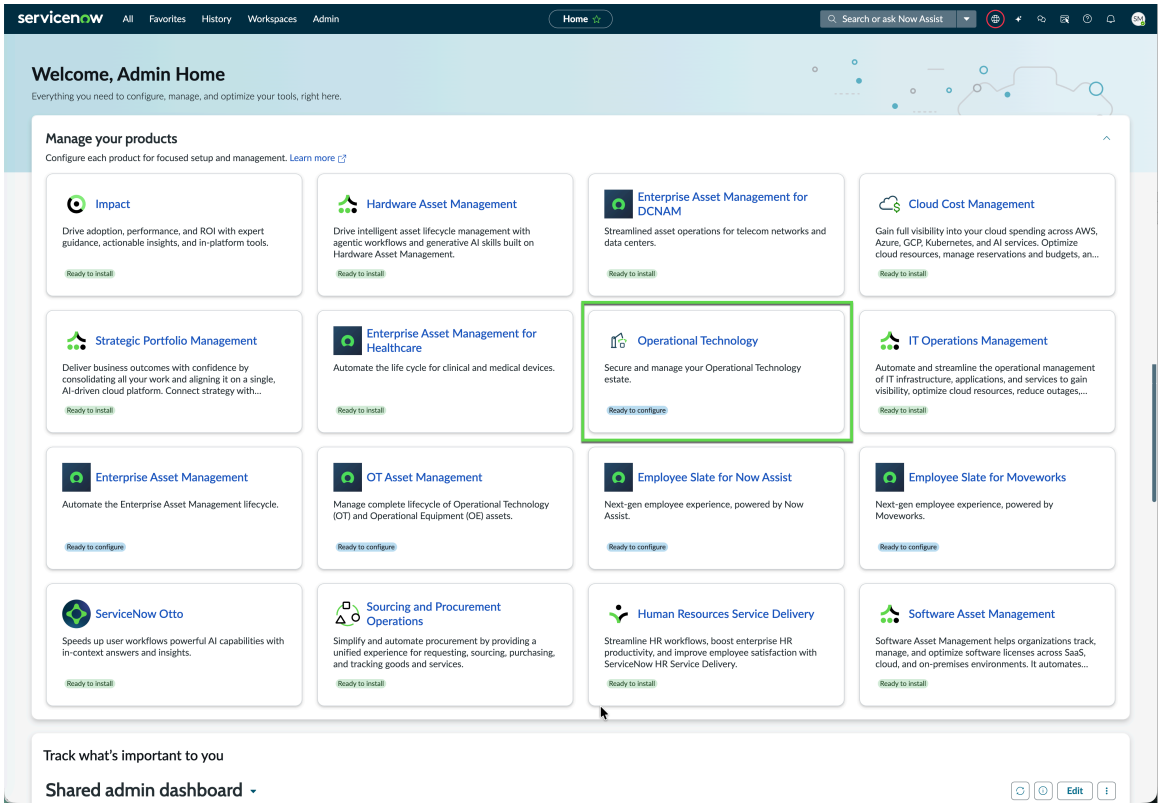
Before you begin

Role required: admin

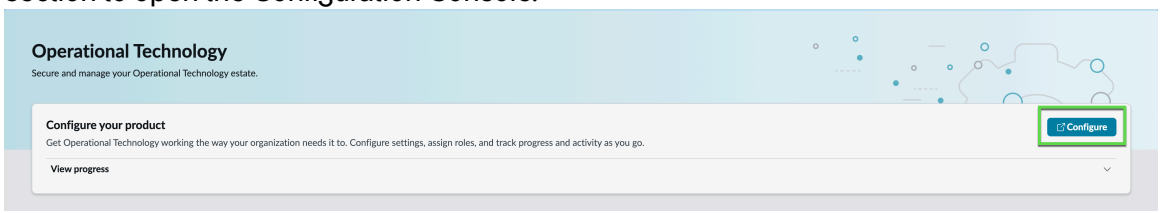
Procedure

1. Access the Admin Home by logging in to your instance or navigating to **All** > **Admin Center** > **Admin Home**.
2. Locate and select the **Operational Technology** card.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. In the Operational Technology Product Hub under the **Apps and plugins** section, install the required OT applications.
4. After the application installation is complete, select **Configure** in the **Configure your product** section to open the Configuration Console.



5. Complete the configuration items listed under **Operational Data**.
   For more information about the OT configuration items, see Operational Technology Setup configuration items.

Use Operational Technology Setup

Complete the configuration items for Operational Technology (OT) to help set up your OT environment.

Operational Technology Setup configuration items

The Configuration Console contains Operational Technology (OT) Setup configuration items, grouped by category, that administrators can complete.

Administrators can access and complete configuration items for user creation, group creation, and user and group role assignments. The following section describes the configuration items included in the Configuration Console under **Operational Data**.

Note: You can also use the ServiceNow Otto panel to help you complete configuration items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

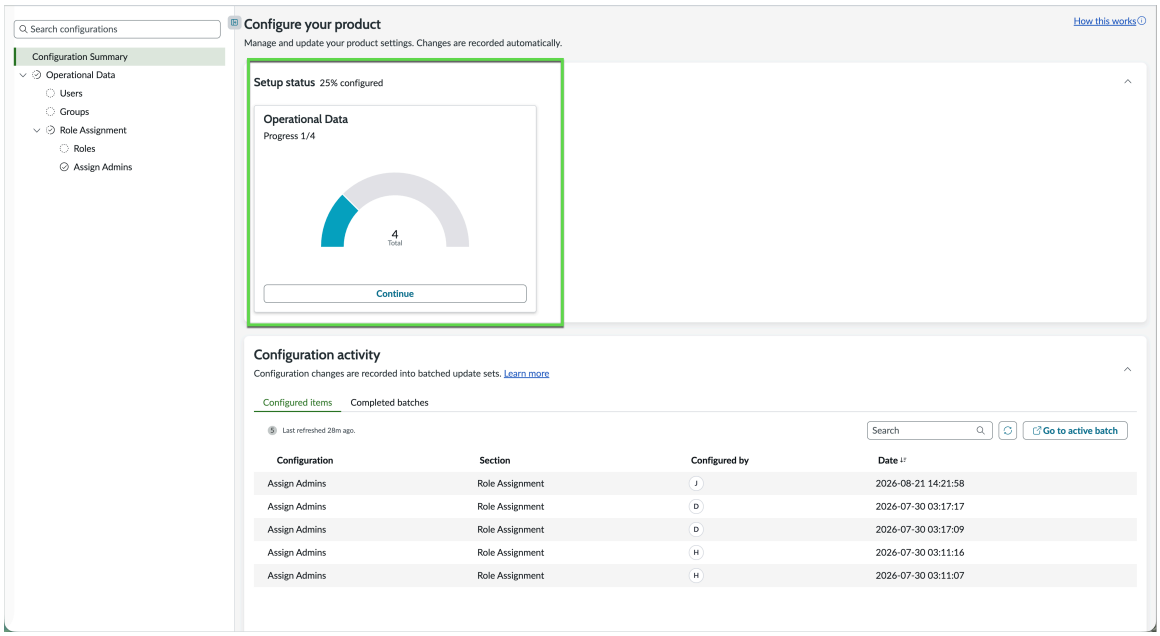
Operational Data

The Operational Data section contains configuration items that organize setup tasks by category.

Operational Data configuration items

Configuration item	Description
Users	• Add and manage users and job titles • Assign groups to users
Groups	Organize users and assign roles using assignment groups.
Role Assignment	
Roles	Specify roles for individuals or groups as needed to provide users access to OT data.
Assign Admins	Assign admin roles to the user or users who manage configuration and operational control.

When you complete each configuration item, you can select **Mark as configured** to update the Setup status available in the Configuration Summary, shown in the following image.



Add OT users with ServiceNow Otto for Setup

Add Operational Technology (OT) users to your system, edit existing users, and assign multiple users to a group.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Access the Admin Home by logging in to your instance or navigating to **All** > **Admin Center** > **Admin Home**.
2. Locate and select the **Operational Technology** card.
3. In the **Configure your product** section, select **Configure** to open the configuration console.
4. In the **Operational Data** section, select **Users**.
5. Edit an existing user's information by selecting the record in the list and updating the user record.
6. To add a user, complete the following steps.

   a. Select **Add a user**.

   b. On the form, fill in the fields as needed.
   For more information about the user form, see Create a user.

   c. Select **Save**, or **Save & add more** to repeat the process and add additional users.

   Alternatively, you can upload a Microsoft Excel spreadsheet with user information by selecting the **Add a user - More actions** icon, selecting **Upload users**, and following the procedure on the **Import external data into User** page.
7. To add users to a group, complete the following steps.
   a. Select the check box next to the user or users to add to a group.
   b. Select **Assign groups**.
   c. Search for and select one or more groups as needed.
   d. Select **Update**.
8. After creating, editing, and adding users to groups as needed, select **Mark as configured**.

What to do next
Add an OT group with ServiceNow Otto for Setup

Add an OT group with ServiceNow Otto for Setup

Add an Operational Technology (OT) group so you can organize users and assign roles per group.

Before you begin
Role required: admin

Procedure

1. Access the Admin Home by logging in to your instance or navigating to **All** > **Admin Center** > **Admin Home**.
2. Locate and select the **Operational Technology** card.
3. In the **Configure your product** section, select **Configure** to open the configuration console.
4. In the **Operational Data** section, select **Groups**.
5. Edit an existing group's information by selecting the record in the list and updating the record.
6. To add a group, complete the following steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Alternatively, you can upload a Microsoft Excel spreadsheet with group information by selecting the **Add a group - More actions** icon, selecting **Upload groups**, and following the procedure on the **Import external data into Group** page.

a. Select **Add a group**.

b. On the form, fill in the fields as needed.
For more information about the group form, see Create a user group.

c. Select **Save**, or **Save & add more** to repeat the process for additional groups.

7. To assign one or more roles to a group, complete the following steps.
   a. Select the check box next to the group or groups to assign a role to.
   b. Select **Assign roles**.
   c. Search for and select one or more roles as needed.
   d. Select **Update**.
8. After creating groups and assigning roles as needed, select **Mark as configured**.

What to do next
Assign OT roles to a user or group with ServiceNow Otto for Setup

Assign OT roles to a user or group with ServiceNow Otto for Setup

Assign Operational Technology (OT) roles to a user or group as needed so that group members can access the data required for their work.

Before you begin
Role required: admin

Procedure
1. Access the Admin Home by logging in to your instance or navigating to **All** > **Admin Center** > **Admin Home**.
2. Locate and select the **Operational Technology** card.
3. In the **Configure your product** section, select **Configure** to open the configuration console.
4. In the **Operational Data** section, expand the **Role Assignment** module and select **Roles**.
5. Select the check box next to the role or roles to assign.
6. Select **Assign groups**.
7. Search for and select one or more users or groups as needed.
8. Select **Update**.
   Any roles already assigned to the selected user or group are skipped.
9. When you're finished assigning roles, select **Mark as configured**.

Result
If all role assignments are successful, you see a `Roles assigned successfully` alert.

If there are errors during the role assignment process, you will see an alert. For more information about error causes and alerts for OT Setup, see Role assignment alerts for Operational Technology Setup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
Assign OT admin roles with ServiceNow Otto for Setup

Assign OT admin roles with ServiceNow Otto for Setup

Create users and assign the necessary Operational Technology (OT) admin roles to users managing configuration and operational control.

Before you begin
Role required: admin

Procedure

1. Access the Admin Home by logging in to your instance or navigating to **All** > **Admin Center** > **Admin Home**.
2. Locate and select the **Operational Technology** card.
3. In the **Configure your product** section, select **Configure** to open the configuration console.
4. In the **Operational Data** section, expand the **Role Assignment** module and select **Assign Admins**.
5. In the **User** field, search for and select the admin user to assign an OT admin role to.
6. In the **Roles** field, select one or more admin roles as needed.
   The Implementation Agent (sn_ia_config.ia_user) role and at least one admin role are required to complete this step.
7. Select **Assign roles**.
   Any roles already assigned to the selected user are skipped.
8. When you're finished assigning admin roles, select **Mark as configured**.

Result
If all role assignments are successful, you see a `Roles assigned successfully` alert.

If there are errors during the role assignment process, you will see an alert. For more information about error causes and alerts for OT Setup, see Role assignment alerts for Operational Technology Setup.

Operational Technology Setup reference

Reference topics provide additional information about the Operational Technology Setup application.

Role assignment alerts for Operational Technology Setup

If there are errors during the role assignment process for Operational Technology (OT) Setup, an error message appears that describes the cause.

Error alerts

Error cause	Alert
Selected group or user already has all the necessary roles.	**Roles already assigned**. The user assigned all the necessary roles.
A role assignment failed.	**[Role name] roles couldn't be assigned**. Please try again.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Error alerts (continued)

Error cause	Alert
No user is selected.	**No user selected**. Select at least one user before assigning roles.
Role assignment process is stuck due to an unexpected error.	**Something went wrong**. An unexpected error occurred while assigning roles.
During OT admin role assignment, an admin role isn't selected.	**Only the Implementation Agent (sn_ia_config.ia_user) role is selected**. Please select at least one of the OT Admin roles to get started.

Operational Technology Manager

The Operational Technology Manager application creates the foundational data and relationships that enable your organization to use the ServiceNow® Operational Technology solution. Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the ServiceNow AI Platform.

Watch an overview about Operational Technology and the ServiceNow Operational Technology Management solution.

https://player.vimeo.com/video/1136253660?h=6cb04e4c1c&badge=0&autopause=0&player_id=0&app_id=58479

Explore



Learn about how manufacturers use the Operational Technology Manager

Configure



Plan and configure your implementation

Use



Import, discover, and review Operational Technology devices

Integrate



Extend Operational Technology Manager by integrating it with other applications

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reference

Get details about related information and applications

Exploring the Operational Technology Manager

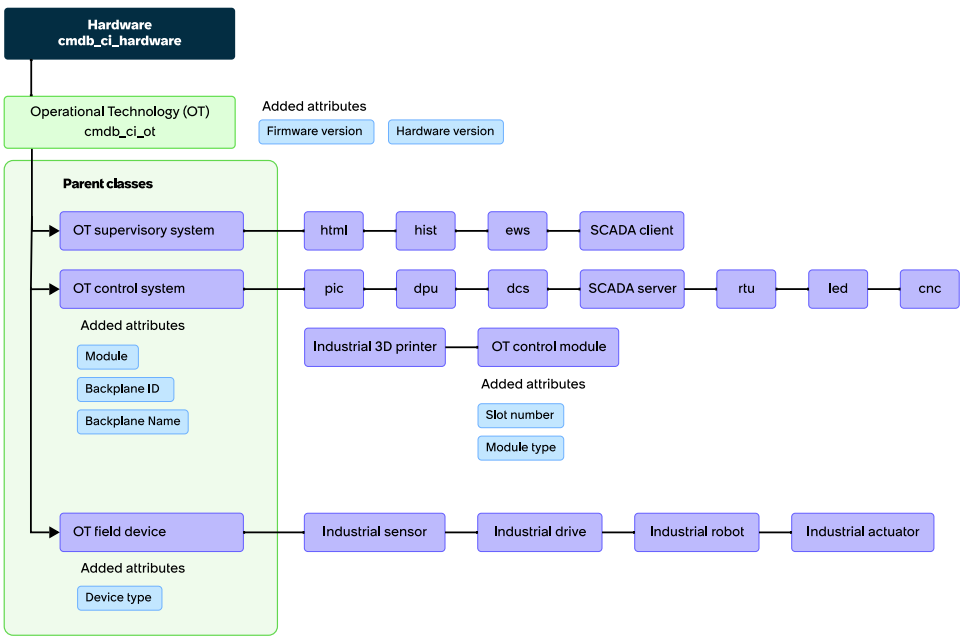
Learn how you can use the Operational Technology Manager application to create the foundational data and relationships that enable your enterprise to use the ServiceNow® Operational Technology solution.

The Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the ServiceNow AI Platform.

Operational Technology Manager (OT) configuration item extension classes

Operational Technology Manager uses Operational Technology (OT) configuration item (CI) extension classes that extend the CMDB class hierarchy as shown in the following figure.

OT CI extension classes equals OT devices



Operational Technology Manager includes class descriptions, identification rules, identifier entries, and dependent relationships, if applicable. The Service Graph applications use these class extensions to populate CIs and discover various technologies and software. To learn more, see Operation Technology (OT) extension classes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CMDB CI classes for Operational Technology Manager

Operational Technology Manager adds these Configuration Management Database (CMDB) configuration item (CI) classes that are part of the CMDB CI Class Models application.

Note: To learn more about this application, see the CMDB CI Class Models application in the ServiceNow Store.

CMDB CI Classes for Operational Technology Manager Workflows

Class	Description	CI class extended
Network Intrusion Detection System	The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.	cmdb_ci_nids

OT device data import and discovery

Multiple methods are available for uploading your existing Operational Technology device data into the ServiceNow AI Platform.

Service Graph Connector (Excel)

You can use the Service Graph Connector (Excel) function to import your Operational Technology data from a populated Microsoft Excel flat-file spreadsheet. You use the spreadsheet in the Integration Hub Extract Transform Load (ETL) to upload this data to the CMDB. To learn more, see Service Graph Connector for Microsoft Excel.

Discovery for Operational Technology

To discover Operational Technology devices in designated Purdue levels in your Industrial Control System (ICS) networks, you run the Discovery for Operational Technology function on a recurring basis. It operates in a manner that is similar to the standard Discovery processes. However, its Discovery normally takes place in the Purdue levels 3 through 3.5, depending on which level you select when you create an OT discovery schedule. To learn more, see IT Discovery for Operational Technology (OT) Networks.

Note: To learn more about Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.

Service Graph Connectors from ServiceNow partners

ServiceNow partners also offer Service Graph Connectors that you can use to upload your existing OT data.

Differences between OT and standard IT networks

There are differences in how the Configuration Management Database (CMDB) handles the devices located in Operational Technology networks and those in standard Information Technology (IT) networks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuration items (CIs) managed under Information Technology Operations Management (ITOM) are classified as type IT in the CMDB. They exist in Levels 4 and 5 of the Purdue Model, or at the Enterprise level.

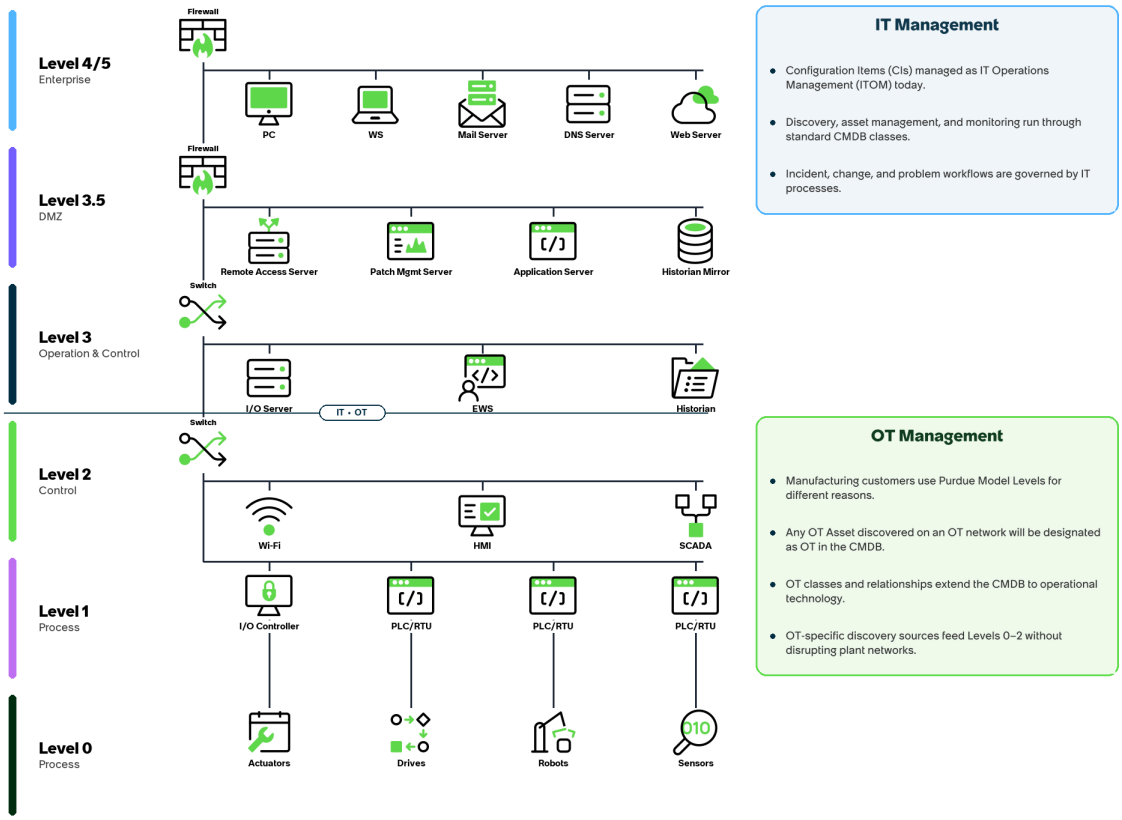
Devices managed under the OT data model exist in Levels 0 to 3.5 of the Purdue Model, and there are two primary components of OT devices:

1. A CI class record. This can be an IT or an OT class CI.
2. An OT device details record. This describes the OT device type (function) and other OT-specific attributes.

Note: For more information about the OT data model and extension classes, see Operational Technology (OT) extension classes.

The following graphic depicts these differences.

Operational Technology CMDB Class Models support Purdue levels



Note: To learn more about Purdue levels, see Industrial Control Systems.

Operational Technology (OT) Manager Foundation

The Operational Technology (OT) Manager Foundation plugin uses generative AI to help streamline processes in the Industrial Workspace related to your OT device data. You can search for OT devices with the OT Configuration Management Database (CMDB) search feature and use an agentic workflow to automate the OT device import process.

OT Manager Foundation overview

With generative AI skills and agentic workflows, you can use the following features of the OT Manager Foundation:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- An OT CMDB search feature that enables you to search for OT configuration item (CI) information and OT device information.
- An OTM agentic workflow that automates the import and validation of your OT device data into the OT CMDB.

Note: Depending on your license, you will have access to certain application features, generative AI skills, agentic workflows, and AI agents. For more information, see ServiceNow product tiers.

Availability notices

Important:

- Not all model providers are available for customers with in-country SKUs, and some AI products/features are currently unavailable for in-country customers. For more information, see the KB1584492 article in the Now Support Knowledge Base. Be sure to check for model provider availability updates in future releases.
- Some AI products/features are currently unavailable for customers in the FedRAMP, NSC DOD IL5, or Australia IRAP-Protected data centers, self-hosted customers, or in other restricted environments. For more information, see the KB0743854 article in the Now Support Knowledge Base. Be sure to check for availability updates in future releases.
- Some AI products/features are currently available only for customers in some regions. Be sure to check for availability updates in future releases.
- Some AI products and skills are not available in Regulated Markets. For more information, see KB2593939: Regulated Markets AI Products/Skills Not Available. Be sure to check for availability updates in future releases.

Troubleshoot and get help

- ServiceNow Community on AI and Intelligence
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

AI limitations

This application uses artificial intelligence (AI) and machine learning, which are rapidly evolving fields of study that generate predictions based on patterns in data. As a result, this application may not always produce accurate, complete, or appropriate information. Furthermore, there is no guarantee that this application has been fully trained or tested for your use case. To mitigate these issues, it is your responsibility to test and evaluate your use of this application for accuracy, harm, and appropriateness for your use case, employ human oversight of output, and refrain from relying solely on AI-generated outputs for decision-making purposes. This is especially important if you choose to deploy this application in areas with consequential impacts such as healthcare, finance, legal, employment, security, or infrastructure. You agree to abide by ServiceNow's AI Acceptable Use Policy, which may be updated by ServiceNow.

Data processing

This application requires data to be transferred from ServiceNow customers' individual instances to a centralized ServiceNow environment, which may be located in a different data center region from the one where your instance is, and potentially to a third-party cloud provider, such as Microsoft Azure. This data is handled per ServiceNow's internal policies and procedures, including our policies available through our CORE Compliance Portal.

Data collection

ServiceNow collects and uses the inputs, outputs, and edits to outputs of this application to develop and improve ServiceNow technologies including ServiceNow models and AI products. In addition, this application will collect incident data (for Incident Assist and Knowledge Assist) and chat transcripts (for Chat Assist). Customers can opt out of future data collection at any time, as described in the Now Assist Opt-Out page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information, see the Now Assist documentation.

Enhanced Access Control for Operational Technology

Enhanced Access Control for OT implements data filters, deny unless access control rules (ACLs), and ACL query rules to help promote system security. Granular access control extends these protections to the Equipment Model Entity (EME) level, so you can restrict access from the site level to individual plants, lines, areas, and other ISA 95 hierarchy nodes.

Enhanced Access Control overview

Enhanced Access Control provides the following components to provide access control configurations for your data to help avoid misconfiguration and security issues.

Data filers

Ability to control access at the query level.

Deny Unless ACLs

Ability to deny access to data unless the specific conditions are met.

ACL Query Rules

Exact query and range query ACL operations to control query privileges.

Enhanced Access Control for OT

Deny Unless ACLs help enforce IT and OT separation and site-based access.

IT and OT separation

Non-OT users can't view OT devices in Configuration Management Database (CMDB) tables. If a device is classified as an OT CI, only users assigned the **cmdb_ot_viewer** role, or the **cmdb_ot_editor** role can access it. The following table describes each role.

OT roles to view OT CIs

Role	Description
OT Viewer [cmdb_ot_viewer]	Read-only access to OT device records.
OT Editor [cmdb_ot_editor]	Create, read, update, and delete access for Operation Technology (OT) extension classes. **Note:** Users assigned the **cmdb_ot_editor** role can edit and delete only OT configuration items (CIs) and can't edit IT CIs.

There are also restrictions on OT users who can edit or delete IT configuration items (CIs). Users assigned the **cmdb_ot_editor** role, or the **cmdb_ot_admin** role can't edit or delete IT CIs in the following related lists:

- IP Address
- Network Adapter
- Storage Device
- File System
- Memory Module

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Patch = CI Field
- Package = CI Field
- Managed Network

Site-based access

Site-based access specifies which users can view, edit, and delete OT devices for a designated site. You can assign site-based access to users by using Can Read or Can Edit user criteria. For more information about assigned Can Read access, see Assign user criteria for Can Read access to a site. For more information about assigning Can Edit access, see Assign user criteria for Can Edit access to a site.

The following table describes the site-based access for users assigned the **cmdb_ot_viewer** role or the **cmdb_ot_editor** role.

Site-based access for OT roles

Role	Site-based permission
cmdb_ot_viewer	With Can Read access, users assigned the **cmdb_ot_viewer** role can only view OT devices for a designated site. For example, if you're assigned the **cmdb_ot_viewer** role and have Can Read access to the Atlanta site, then you can only view the site's OT devices. You can't edit or delete the OT devices associated with Atlanta.
cmdb_ot_editor	To edit OT devices, users with the **cmdb_ot_editor** role should be assigned Can Edit access for the site, or sites they belong to. For example, if you're assigned the **cmdb_ot_editor** role but only have Can Read access to the Atlanta site, you can only view the devices associated with Atlanta. If you're assigned the **cmdb_ot_editor** role and have Can Edit access to the San Diego site, you can edit or delete the devices associated with San Diego.

Granular ACL extends access

Site-based access controls access at the site level. Granular access control extends permissions to individual Equipment Model Entities (EMEs) within a site — such as plants, lines, areas, and cost centers. Use granular access control to scope access to the exact ISA 95 hierarchy nodes for which each user or group is responsible.

Important:

New records can't be created directly on the `isa_entity_user_criteria_access` table through the UI or any insert path. Existing records on this table remain readable and can be updated per the applicable ACL.

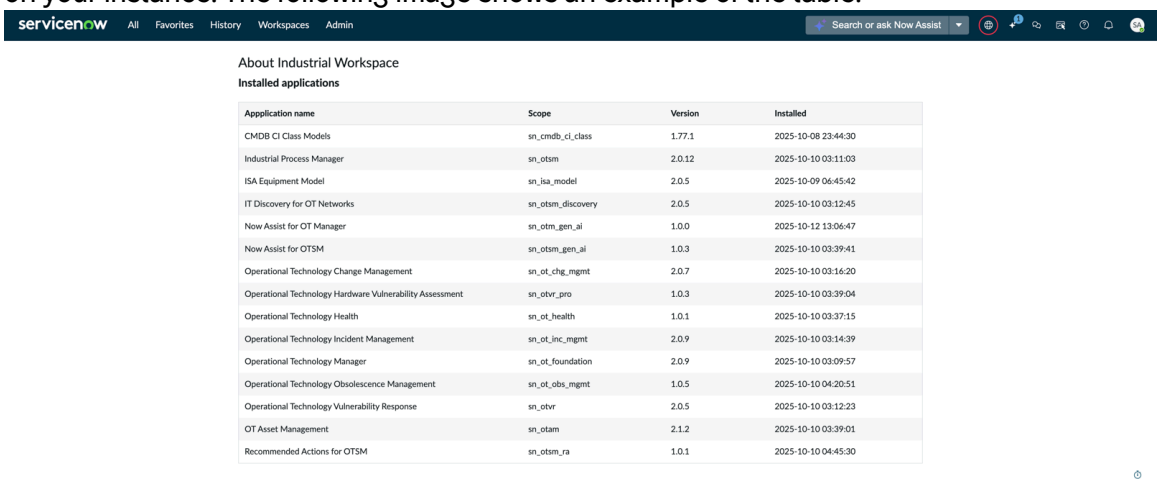
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Viewing your installed Operational Technology applications

You can view the Operational Technology (OT) applications that you have installed on your instance for better visibility of how you can use the Operational Technology Management solution.

If you're assigned the cmdb_ot_viewer or cmdb_ot_isa_viewer role, you can view the OT applications that you have installed on your instance by navigating to **All** > **Industrial Workspace Admin** > **About Industrial Workspace**.

The Installed applications table contains the application name, scope, version, and install date for each application installed and available on your instance. The following image shows an example of the table.



Configuring the Operational Technology Manager

Configure the Operational Technology Manager application so that you can create the data foundation for the ServiceNow® Operational Technology solution.

Task	Purpose
1. Install Operational Technology (OT) extension classes.	Extend the Configuration Management Database (CMDB) class hierarchy for use in Operational Technology processing.
2. Install Operational Technology Manager.	Install the Operational Technology Manager application.
3. Assign Operational Technology roles.	Assigns roles to control the actions that are available for each user.
4. Prepare a Microsoft Excel spreadsheet for Service Graph Connector import.	Create and populate a Microsoft Excel spreadsheet with your existing Operational Technology data for upload to the ServiceNow AI Platform. For more information, see Prepare your Pre-import OT Worksheet Entry Review tool for Service Graph Connector import.
5. Import your Excel spreadsheet with an import task.	Upload your Operational Technology data to the Configuration Management Database (CMDB).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Purpose
	For more information, see Using the Service Graph Connector for Microsoft Excel through import tasks.
6. Run the IT Discovery for OT Networks function.	Discover Operational Technology (OT) devices in the designated Purdue levels in your Industrial Control System (ICS) networks. For more information about Discovery for Operational Technology, see IT Discovery for Operational Technology (OT) Networks.
7. Install Service Graph Connectors that are provided by ServiceNow® partners.	Install ServiceNow, Inc. connectors that are provided by partners as they become available in the ServiceNow® Store.
8. Use the **All OT Devices** or **All OT Devices by IP Address** selections on the **Operational Technology (OT)** menu.	Edit or view detailed information for the OT devices in your enterprise, after you've imported your Excel spreadsheet, or have run the IT Discovery for OT Networks function.

Implementing the CSDM framework for Operational Technology

Following the CSDM framework ensures that you meet your primary goal of consistent accuracy in reporting and analytics so that you can effectively manage your Operational Technology (OT) environment.

CSDM framework for OT

You must complete the implementation for the CSDM framework in stages. For more information, see Implementing the CSDM framework in stages.

Operational Technology product view

Operational Technology covers products that tackle aspects of managing OT devices and production processes at various stages of the life cycle. The goal of this product view is to help you to understand how Operational Technology key entities work with the core Common Service Data Model (CSDM) framework.

Operational Technology Manager

Creates the foundational data and relationships that enable your enterprise to use the Operational Technology solution. For more information, see Operational Technology Manager.

Industrial Process Manager

Enables you to create the ISA-95 Equipment Model data foundation that is required for the Operational Technology solution. For more information, see Industrial Process Manager.

Operational Technology Discovery

Enables you to discover and map OT devices and assets in your operational technology environment. For more information, see Operational Technology Discovery.

Operational Technology Vulnerability Response

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Enables effective prioritization and remediation of OT device vulnerabilities at the site level. For more information, see Operational Technology Vulnerability Response.

Operational Technology Incident Management

Enables engineers to quickly resolve OT device and production process issues. For more information, see Operational Technology Incident Management.

Operational Technology Change Management

Enables your organization to implement changes to OT devices and production processes. For more information, see Operational Technology Change Management.

Operational Technology Knowledge Management

Enables your organization to capture information about your OT system in knowledge articles that are related to OT incidents. For more information, see Operational Technology Knowledge Management.

Operational Technology Request Management

Enables you to access the OT Service Catalog to request OT catalog items and fulfill them based on the defined flows. OT workers can then create and submit an OT request from a catalog item, which helps provide a consistent experience and facilitates cross-functional requests. For more information, see Operational Technology Request Management.

Recommended Actions for Operational Technology Service Management (OTSM)

Allows you to set up and apply real-time actionable recommendations for speeding up the triaging process and resolving issues quickly across various records in the Industrial Workspace, including OT incidents. For more information, see Recommended Actions for Operational Technology Service Management (OTSM).

AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

Accesses external sources related to an OT incident, and contextualizes how the document is relevant to the incident. For more information, see AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM).

Employee Center for OT

Provides a central location where you can submit requests related to OT and industrial services. For more information, see Employee Center for OT.

Industrial Workspace

Provides OT users with the tools they need to manage their OT data. For more information, see Industrial Workspace.

Operational Technology and CSDM tables

Operational Technology manages and uses CSDM tables. Several ServiceNow products benefit from and add value to Operational Technology.

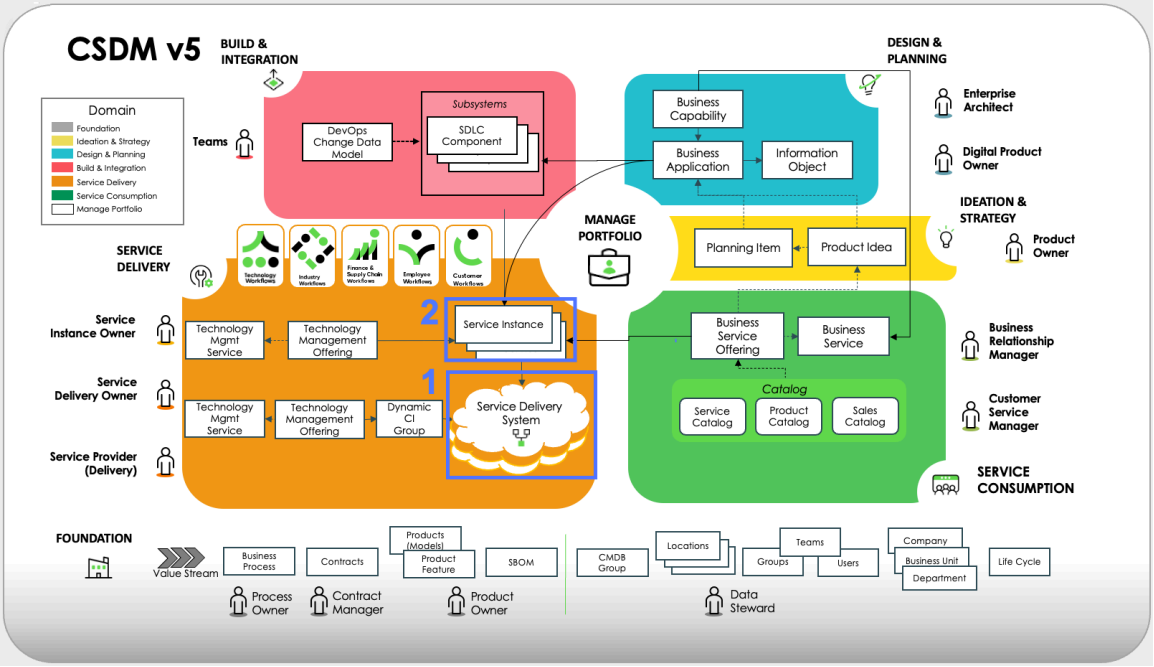
CSDM tables managed by Operational Technology

There are three primary categories of tables managed by Operational Technology (OT):

- Operational Technology devices: Configuration items found on an OT (ICS or PCN) network.
- ISA equipment model entity: Industrial process automated by OT devices.
- OT system service: Creates other control systems, such as a distributed control system (DCS).

The numbers in this figure correspond to the CSDM tables managed by Incident Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



CSDM tables used by Operational Technology

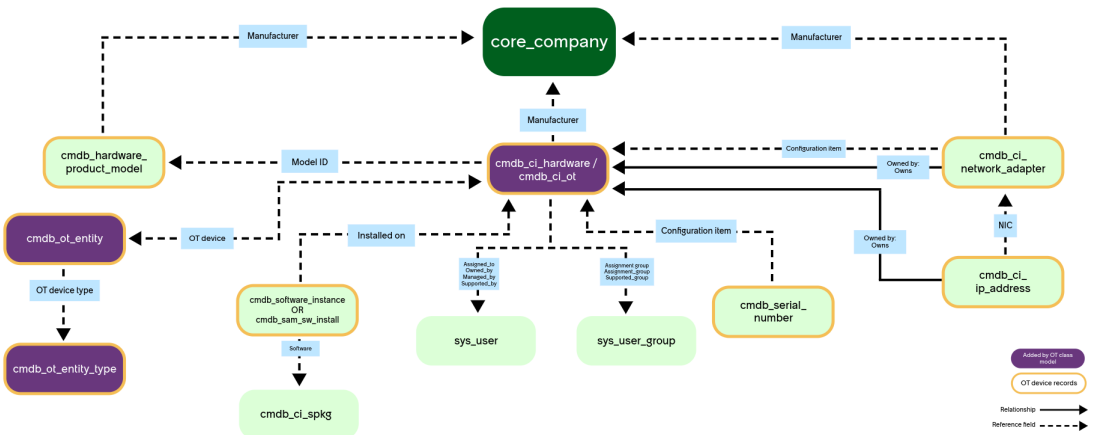
1. OT devices:

a. Configuration Item classes were created for Operational Technology hardware classes (cmdb_ci_ot) by extending hardware. See Operational Technology (OT) extension classes for details.

b. Any CI Class (any relevant existing hardware class as well as new OT classes) can be designated as OT devices. This can be achieved by adding OT device details using the OT Device Details (cmdb_ot_entity) reference to the cmdb_ot_entity table. OT Device Details include OT-specific characteristics like Purdue Level and OT device type.

c. OT device types describe the function of any CI that automates an industrial or production process. The cmdb_ot_entity_type table describes these functions or roles.

As shown here, a single OT device is represented by at least two records: one CI and one OT entity record. The device can contain six or more records in up to six tables (for example, if the CI has more than one IP and MAC address).



2. Equipment model entities:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. The equipment model entity class extends the Calculated Application Service and is used to:

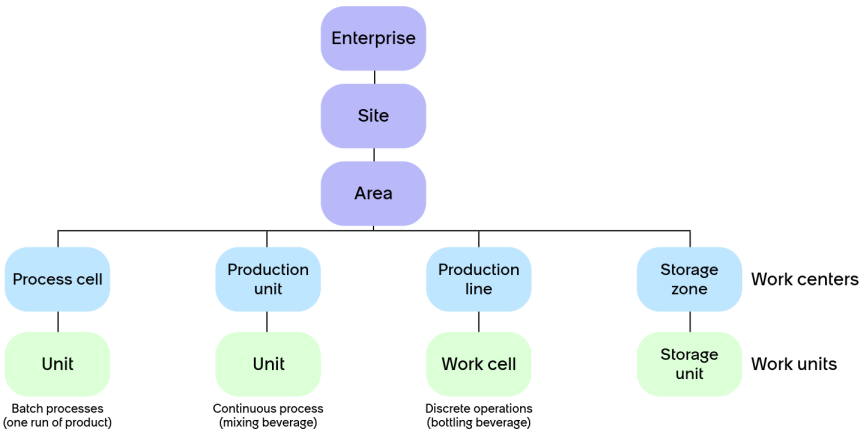
i. Represent the site of any OT device or equipment model entity. A record in the Equipment Model Entity table (cmdb_ci_ot_isa_entity) without a parent is considered a site.

ii. Represent the ISA equipment model entity for a part of the production process.

b. You can use equipment model templates (isa_entity_template) to further describe the relationships between equipment model entities found in an industrial environment.

i. Levels (isa_entity_level) describe the hierarchical level of the equipment model entity. For the default ISA-95 template, the levels shown here (area, work center, and work units) are included in the base system.

ii. Level types (isa_entity_type) describe the type of process represented by the equipment model entities at a given level. For the default ISA-95 template, the types shown here (process cell, production unit, production line, and storage zone) are included in the base system.



3. OT system service:

a. The OT system service class extends the Calculated Application Service and is used to create the OT system service

b. The OT system service can then be associated with equipment model entities, technical services for software applications, and business offerings.

c. The OT system service can be related to the following items:

- OT devices that are part of the OT system service
- Equipment model entities that the OT system service manages

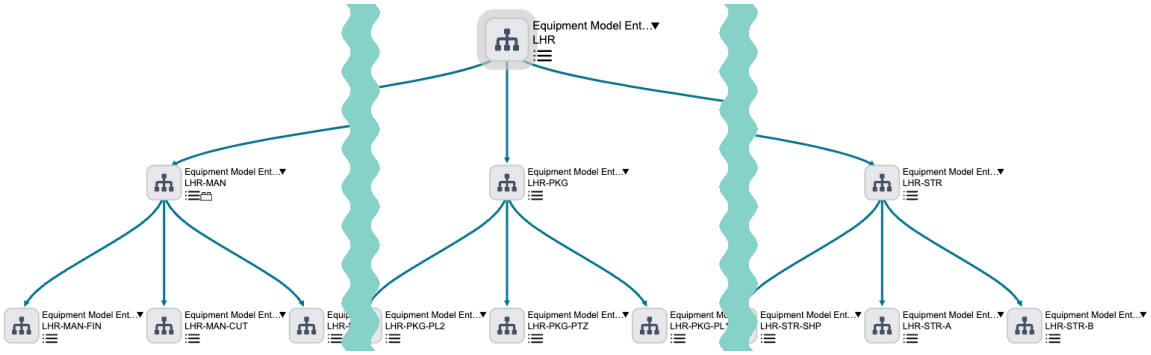
CSDM includes relationship types (specific to Operational Technology) that more accurately distinguish how OT devices and equipment model entities relate to each other:

- **Producer for::Consumer of**: Describes the production process (material flow) between equipment model entities.
- **Contains Element::Element of**: Describes the hierarchical relationship between equipment model entities.
- **Automated by::Automates**: Describes the relationship between an OT device and an equipment model entity that the OT device automates.

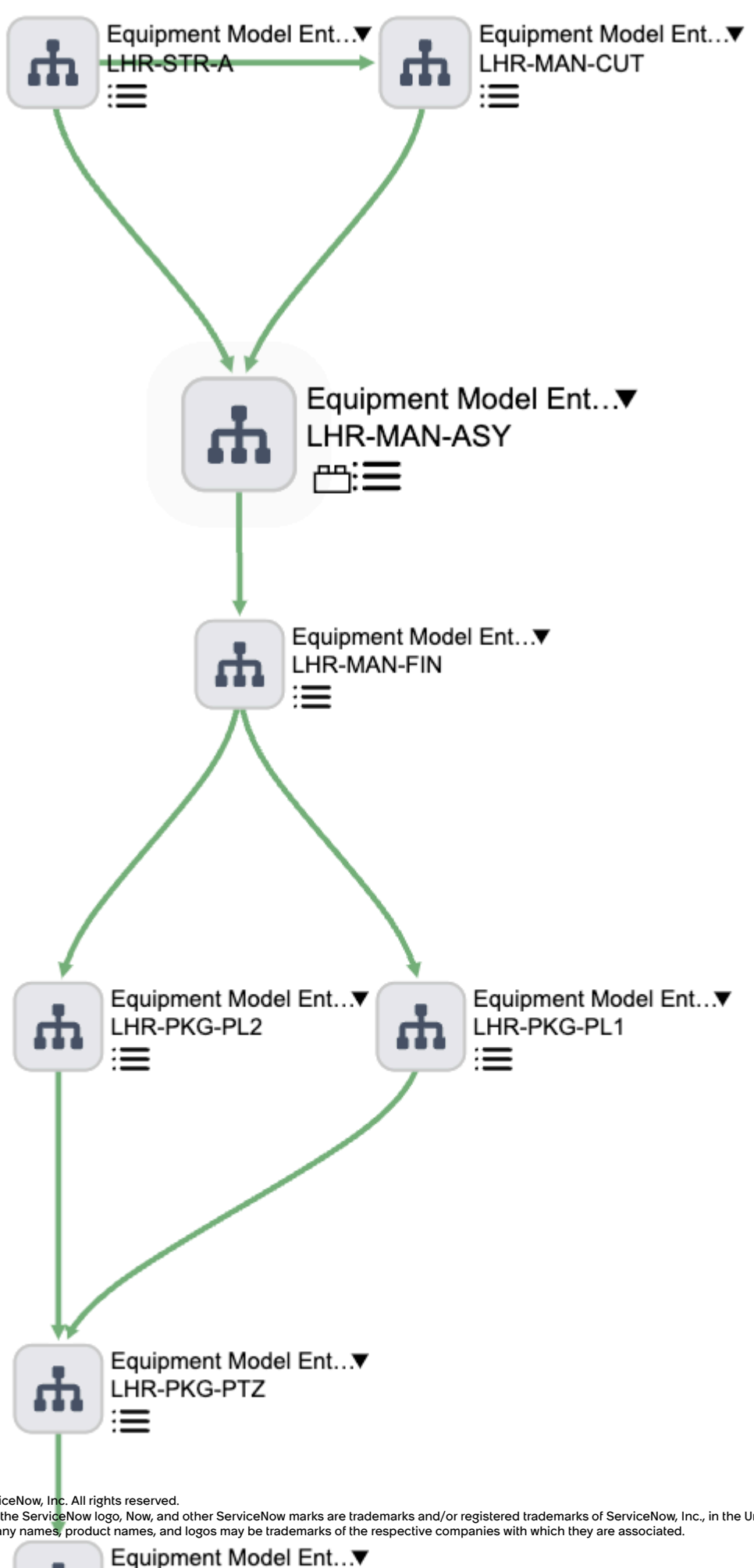
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Detects::Detected by**: Describes which Network Intrusion Detection System (NIDS) class (cmdb_ci_nids) detected an OT device on an OT network.
- **Owns::Owned by**: Describes the relationship when an OT Control Module is owned by an OT Control System (PLC, DCS, and so on)

The following dependency maps show the relationships between OT devices and equipment model entities:



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Products that add value to Operational Technology

When you use OT with any of the following ServiceNow products, you increase the value you get from OT.

Discovery for Operational Technology

Discovery for Operational Technology provides details about IT-classed hardware and software CIs. It can be configured to provide additional OT device context like Purdue Level and Site on a per-OT schedule basis. Discovery for OT is part of the Operational Technology Manager product.

Industrial Process Manager

When OT devices are assigned to an equipment model entity, *automated by::automates* relationships are created between them. This can be done manually in the Industrial Workspace. You can also use the Automatic Mapping Across Zone-based IP Network Groups (AMAZING) feature in the OT Subnet Mapping menu item. This feature establishes a relationship between OT subnets and equipment model entities.

Operational Technology Vulnerability Response

When vulnerable item (VIT) records are created by importing records from an OT-certified integration with a third-party security platform, OT devices are associated with the VIT. This enables both of the following capabilities:

- Risk calculation based on the criticality of the mapped equipment model entity.
- Assignment of VITs to the appropriate local team for remediation via site-based assignment groups.

Operational Technology Incident Management

Incident Management for OT runs separately from IT for most OT devices. OT incident records enable site-based access and views to issues that are related to OT devices.

Operational Technology Change Management

OT change requests enable changes to OT devices or industrial equipment configurations.

Operational Technology Knowledge Management

Operational Technology Knowledge Management enables you to capture information about your OT system in knowledge articles that are related to OT incidents.

Operational Technology Request Management

Enables you to access the OT Service Catalog to request OT catalog items and fulfill them based on the defined flows. OT workers can then create and submit an OT request from a catalog item, which helps provide a consistent experience and facilitates cross-functional requests.

Products that benefit from Operational Technology

IT Service Management (ITSM)

Services have the context of the site, production process, and OT devices, along with the information and technologies layered beneath them.

Information Technology Operations Management (ITOM)

Understands the business context for the production processes along with the OT device hardware and software being managed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Security Operations

Understands the business context for the production processes as well as OT device hardware and software being secured.

Governance, Risk, and Compliance (GRC)

Auditors can better leverage production process flows and related Information objects. This helps auditors understand the design-time data sensitivity for scoping audits, measuring risks, and managing audit activities.

Asset Management

Manages the impact of the software and hardware life cycle process on the production processes.

Operational Technology Manager use case

The Operational Technology Manager use cases are described in this section.

Operational Technology Manager use case

The Operational Technology Manager application creates the foundational data and relationships that enable your enterprise to use the Operational Technology solution. It supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the ServiceNow AI Platform.

The OT Visibility dashboard in the Industrial Workspace summarizes your OT device inventory. For more information about the dashboard, see Operational Technology Visibility dashboard.

Key features

- Operational Technology Manager uses OT configuration item (CI) extension classes that extend the CMDB class hierarchy.
- IT Discovery for OT Networks is restricted to OT specific roles and OT related meta data can be added to an OT discovery schedule.
- The Service Graph connector (Excel) imports OT data from a populated Microsoft Excel flat-file spreadsheet. This data is validated and then transformed into the appropriate table records and relationships to represent OT device details in the CMDB.

Results

With the Operational Technology Manager use case, you can:

- Visualize dependencies of OT devices in the industrial environment.
- Manage the life cycle of OT devices on a site-by-site basis with site specific RBAC
- Create a solid data foundation and define critical levels of infrastructure.

Industrial Process Manager use case

Use the Industrial Process Manager application to create the ISA-95 equipment model data foundation that is required for the Operational Technology solution.

Key features

You can perform the following operations in the Industrial Process Manager workspace:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Use ISA-95 models to describe the production process at each site in the industrial environment.
- Manage equipment model entities and their relationships with each other and with OT devices.
- Automatically map the relationship of all OT devices to the equipment model entity it automates using the OT subnet to equipment model entity relationship.

Results

The Industrial Process Manager enables you to create a custom version of the equipment models in each of your sites.

Operational Technology Vulnerability Response use case

Operational Technology Vulnerability Response enables you to effectively prioritize and remediate OT device vulnerabilities at the site level.

Key features

- Remediation owner workspace maps vulnerable items (VITs) with the production process.
- Risk calculation for OT VITs can be based on criticality of the equipment model entity automated by the OT device.
- Automatic assignment of VITs to remediation owners based on the site assigned to the OT device with the VIT.

Results

By leveraging the CMDB relationships of OT devices, you can prioritize vulnerable devices or items based on the criticality of the production process they automate.

As an OT engineer or OT vulnerability manager, Operational Technology Vulnerability Response enables you to find answers to questions such as:

- What are my OT device vulnerabilities?
- How can I prioritize vulnerability remediation using OT specific risk?
- What progress are we making toward remediation of OT vulnerabilities?

The OTVR (PA) dashboard and the OT Vulnerability Risk Management dashboard in the Industrial Workspace summarize the vulnerabilities in your system. For more information about the OTVR (PA) dashboard, see Operational Technology Vulnerability Response (PA) dashboard. For more information about the OT Vulnerability Risk Management dashboard, see Operational Technology Risk Management dashboard.

Operational Technology Incident Management use case

OT incidents occur when there is a disruption in service that is provided by an OT device on an OT network. Sometimes, the OT device may not be known when the incident is first created. Operational Technology Incident Management enables engineers to quickly resolve OT device and production process issues.

Key features

When you create an OT incident from the Industrial Workspace, the incident is automatically assigned a Network Type of OT to distinguish an OT incident from an IT incident. The field is not displayed by default.

Results

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Incident Management enables engineers to quickly resolve OT device and production process issues. It enables you to manage OT incidents separately from IT incidents.

Operational Technology Change Management use case

Operational Technology Change Management enables your team members to work collaboratively on changes to OT devices or industrial equipment configurations.

Key features

- Digitized change workflow that connects all stakeholders.
- Sites that have different change management processes (workflows).
- Separated IT Change Management and Operational Technology Change Management, but ability to be combined if necessary.
- Integrated Operational Technology Change Management workflow with the Operational Technology Incident Management and Operational Technology Vulnerability Response applications.
- Aligned factory floor changes for the equipment model entities with downtime schedules.

Results

The following examples show how to apply Operational Technology Change Management to your organization:

- An OT remediation owner, who's responsible for fixing vulnerabilities on OT devices, wants to initiate a change to fix a group of vulnerabilities.
- An OT technician, who's responsible for OT configurations and plant engineering activities, wants to execute a change to fix a malfunctioned robotic arm on the industrial floor.
- A plant head, who's responsible for overall production activity, wants to review and approve a change requested by the engineering team.

Operational Technology Knowledge Management use case

Operational Technology Knowledge Management helps you to capture information about your Operational Technology (OT) system in knowledge articles that are related to OT incidents. Your organization can then use these knowledge articles to help your users to access the right information and prevent miscommunication with your users.

Key features

- Ability to use the existing Knowledge Management ServiceNow AI Platform capabilities with the Operational Technology Management solution.
- Ability to browse all knowledge base articles that are related to an OT incident and to create knowledge articles directly from an incident record.
- Ability to configure an OT knowledge base for knowledge managers and knowledge users.
- Ability to create knowledge articles in the Industrial Workspace.
- Ability to request approvals to publish, edit, retire, or delete a knowledge article.
- Ability to edit existing knowledge articles with updated information.

Results

The following examples show how to apply#Operational Technology Knowledge Management to your team:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- An OT engineer with several years of experience wants to capture their OT device knowledge in one place for guide workers and junior technicians.
- Front-line workers and technicians responsible for production process operations have noticed an issue on the factory floor and need a knowledge article that explains remediation.

Operational Technology Request Management use case

Operational Technology Request Management enables you to access the OT Service Catalog to request OT catalog items and fulfill them based on the defined flows. OT workers can then create and submit an OT request from a catalog item, which helps provide a consistent experience and facilitates cross-functional requests.

Key features

- Provides a single view to efficiently manage multiple catalog requests.
- Encourages transparency, expedites request processes, and minimizes delays with automatic notifications and approvals.
- Maintains the products and services menu that you can use to create and update catalog requests.

Results

The following examples show how to apply#Operational Technology Request Management to your team:

- OT engineers can file and manage OT requests for various OT products and services in a one place.
- A plant head or supervisor can engage with the correct team to remediate an incident reported on the factory floor.

Operational Technology and CSDM elements

Terms related to managing business applications with elements of CSDM.

Operational Technology terms

Term	Definition
Equipment model	The service records that describe how an industrial operation is organized to produce an output or product.
Production process	The relationships between equipment model entities and the various stages of the workflow from the raw material to finished goods.
Site	A parent equipment model entity record that has no parent. This is a special equipment model entity record because it is used to assign read or write level access to the OT devices assigned to the site.
OT device (site assignment)	The site assignment is needed for role-based security (RBAC) of OT devices. This is implemented as a choice list reference field on the OT Device Details (cmdb_ot_entity) table portion of the OT device record because an OT device can belong to only one site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology terms (continued)

Term	Definition
OT device (automates::automated)	The automates::automated by relationship describes how the OT device is related to the production process, which could include more than one equipment model entity.
Windows	In both OT and IT networks, the Windows server is represented in the cmdb_ci_win_server server. Additionally, the Windows server in the OT network has a reference in the cmdb_ci_win_server.cmdb_ot_entity field pointing to a record in the cmdb_ot_entity table that describes its function in OT and other OT characteristics like Purdue Level, site, and so on.

Operational Technology FAQ

You might have questions while implementing the CSDM framework.

What is the difference between a production process and an equipment model entity?

Equipment model entities are the service records used to describe how an industrial operation is organized to produce an output or product. The production process describes the relationships between equipment model entities as material flows from raw input to a finished product.

What is a site?

A site is a parent equipment model entity record that itself has no parent. A site is a special equipment model entity record because it is used to assign read or write level access to the OT devices assigned to the site.

Why does an OT device have both a site assignment and automates::automated by relationships?

The site assignment is needed for role-based security (RBAC) of the OT devices. This is implemented as a choice list reference field on the OT Device Details (cmdb_ot_entity) table portion of the OT device record because an OT device can belong to one site only.

The *`automates::automated by`* relationship describes how the OT device is related to the production process, which could include more than one equipment model entity.

What is the difference between a Windows server found on an OT network and one found on an IT network?

In both types of network, the Windows server is represented in the cmdb_ci_win_server server. Additionally, the Windows server in the OT network has a reference in the cmdb_ci_win_server.cmdb_ot_entity field pointing to a record in the cmdb_ot_entity table that describes its function in OT and other OT characteristics like Purdue Level, site, and so on.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuring the OT Manager Foundation

Configure the features and agentic workflows available for the Operational Technology (OT) Manager Foundation.

Supporting information for OT Manager Foundation

Review language model support, user interfaces, and skill availability for the Operational Technology (OT) Manager Foundation.

Supported language models for all OT Manager Foundation skills and AI agents

You can use Now LLM Service, Azure OpenAI, Google Gemini or Anthropic Claude on AWS as the AI model provider for all generative AI skills and AI agents. Use the Configuration Controls in AI Control Tower to define which options are available, then set the skill-level preferences in the AI Admin Hub console. For more information, see Large language models on the ServiceNow AI Platform.

Supported user interfaces

The OT Manager Foundation includes the features that are listed in the following table.

Note: Depending on your license, you will have access to certain application features, generative AI skills, agentic workflows, and AI agents. For more information, see ServiceNow product tiers.

OT Manager Foundation supported interfaces

Interface	Feature
Industrial Workspace	• Operational Technology (OT) Configuration Management Database (CMDB) search feature to search for OT device records using the ServiceNow Otto panel. The OT CMDB search feature uses the following agentic workflow and skill: ○ ServiceNow Otto for CMDB's Search CMDB agentic workflow. For more information, see Search the CMDB. **Note:** You must have the cmdb_ot_viewer role at minimum to use the CMDB search agentic workflow. ○ ServiceNow AI Platform's Analytics Query Generator skill. For more information, see the Query Generation store listing and Query Generation skills. • Agentic workflow for uploading, importing, and validating your OT device data with the Service Graph Connector for Microsoft Excel.

Activate the OT CMDB Search feature

If you have the admin role, you can configure the Operational Technology (OT) Manager Foundation so that teams can use the OT Configuration Management Database (CMDB) search feature in the Industrial Workspace.

Before you begin
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Use the AI Admin Hub console to configure the OT Manager Foundation. The console helps you install plugins and configure generative AI skills. For more information, see Overview tab in AI Admin Hub.

The following table lists the features and skills that you can access from the AI Admin Hub console.

OTM features and skills in the AI Admin Hub console

OTM features	Skills
Gen AI skills for OTM	Analytics Query Generator

Procedure

1. Install the OT Manager Foundation plugin (sn_otm_gen_ai).
   - For information about the application dependencies, see Supporting information for OT Manager Foundation.
   - For information about the installation process, see Install plugins.
2. Navigate to **All** > **AI Admin Hub**.
3. Select the **AI Skills** tab.
4. Expand the **Data & Analytics** category and select **Analytics**.
5. Find the Analytics Query Generator skill.
6. On the Analytics Query Generator tile, select **Turn on**.

   Important: This generative AI skill is turned on by default. The skill will be automatically available to appropriate role users for the application. For more information, see AI agents, skills, and agentic workflows on by default.

7. In the Turn on skill confirmation window, select **Turn on** to enable the skill.
8. Complete the following steps to display the Search CMDB agentic workflow and your conversation with the agent in the ServiceNow Otto panel.

   Important: This agentic workflow is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

   a. Navigate to **All** > **AI Agent Studio** > **Agentic Solutions**.
   b. In the **Agentic workflows** tab, select the **Search CMDB** agentic workflow.
   c. Open the **Select a UI display** section.
   d. Next to the **ServiceNow Otto panel** option, select the **Display** toggle.
9. Complete the following steps to verify the **Status** toggle is on and confirm the CMDB search AI agent is active and running.
   a. Navigate to **All** > **AI Agent Studio** > **Agentic Solutions**.
   b. In the **AI agents** tab, select the **CMDB CI search AI agent**.
   c. Open the **Toggle display** section.
   d. Select the **Status** toggle if the toggle isn't already selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Activate the Import OT device spreadsheet into OT CMDB agentic workflow

You must activate the agentic workflow from the AI Agent Studio. The Operational Technology (OT) Manager Foundation agent included with the application and used in the agentic workflows is active by default.

Before you begin
Role required: sn_aia.admin

About this task

Important: This agentic workflow is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

Procedure

1. Navigate to **All** > **AI Agent Studio** > **Agentic Solutions**.
2. In the **Agentic workflows** tab, select the **Import OT device spreadsheet into OT** *CMDB* agentic workflow.
3. In the **Define key requirements** screen, review and update the information as needed then select **Save and Continue**.

   Note: In the Define who can access the agentic workflow section for the Import OT device spreadsheet into OT CMDB agentic workflow, a user must have the ot_excel_import_user role to access the agentic workflow.

4. In the **Select a UI display** screen next to the **ServiceNow Otto panel** option, select the **Display** toggle to show the conversation with the agent in the panel.
5. Select **Save and test**.
6. Verify the **Status** toggle is on to confirm the OT Excel import task AI agent is active and running.
   a. Navigate to **All** > **AI Agent Studio** > **Agentic solutions**.
   b. Under the **AI agents** tab, select the **OT Excel import task AI agent**.
   c. In the **Toggle display** screen, select the **Status** toggle if the toggle isn't already selected.

Edit trigger words for OT CMDB search

Edit the trigger words used in the Operational Technology (OT) Configuration Management Database (CMDB) search feature to optimize OT search results.

Before you begin
Role required: admin

About this task
Optionally, update the `sn_mfg_common.ot_cmdb_search_trigger_words` system property to include additional search keywords.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Workspace System Properties**.
2. Under the **OT CMDB Search** section, update the Additional OT CMDB Search trigger words in a comma-separated format (*`sn_mfg_common.ot_cmdb_search_trigger_words`*) system property with additional keywords as needed.

   The following keywords are included for the OT CMDB search feature.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- OT
- Operational Technology
- CNC
- Control system
- Control module
- DCS
- DPU
- EWS
- Field device
- Historian
- HMI
- IED
- OPC client
- OPC server
- PLC
- RTU
- QICS
- Industrial 3D printer
- Industrial actuator
- Industrial drive
- Industrial sensor
- Industrial robot
- Industrial printer
- supervisory system
- SCADA client
- SCADA server

3. Select **Save**.

Operational Technology (OT) extension classes installation

You must install the Operational Technology (OT) extension classes that are the foundation of the Operational Technology Manager.

You can access the OT extension classes by installing the CMDB CI Class Models application. For more information about installation, see CMDB CI Class Models app.

The OT extension class model extend the Configuration Management Database (CMDB) class hierarchy, which includes the following information:

- Class descriptions
- Identification rules
- Identifier entries
- If applicable, dependent relationships

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Applications, such as Discovery and Service Graph Connectors, use these class extensions to populate configuration items (CIs) and discover various technologies and software. For more information about the OT extension classes, see Operational Technology (OT) extension classes.

Install Operational Technology Manager

If you have the admin role, you can install the Operational Technology Manager application. The application includes demo data and installs that are related ServiceNow® Store applications and plugins, if they are not already installed.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.

Note: To learn more about the subscriptions required for the Operational Technology Manager, see Subscriptions for Operational Technology Management (OTM)

Role required: admin

About this task

The following items are installed with Operational Technology Manager:

- Plugins
- Store applications
- Roles
- Tables
- Script includes

For more information on viewing components that are installed with Operational Technology Manager, see Components installed with Operational Technology Manager.

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Operational Technology Manager application using the filter criteria and search bar.

   You can search for the application by its name or ID. If you can't find the application, you might have to request it from the ServiceNow Store.

   Visit the ServiceNow Store to view all the available apps, and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.
3. In the Application installation dialog box, review the application dependencies.

   Dependent plugins and applications appear if they will be installed, are currently installed, or must be installed. If any plugins or applications require installation, you must install them before you can install Operational Technology Manager.
4. **Optional:** If demo data is available and you want to install it, select the **Load demo data** check box.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Demo data are the sample records that describe application features for common use cases. Load the demo data when you first install the application on a development or test instance.

5. Select **Install**.

Assign Operational Technology Manager roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Operational Technology Manager application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the Operational Technology Manager application.

If you want to configure site users, you can create and assign user criteria for equipment model entity site users. For more information, see Manage equipment model site access for non-administrators.

Role	Description
Operational Technology Discovery Administrator [ot_discovery_admin]	Can run the Discovery for Operational Technology process. Can't access the Configuration Management Database (CMDB) to view CIs and related Operational Technology (OT) entities created from discovered items. See Create and run the OT Discovery schedule and the Discovery process.
Operational Technology Manager Viewer [cmdb_ot_viewer]	Read-only access to Operational Technology (OT) device records.
Operational Technology Manager Editor [cmdb_ot_editor]	Create, read, update, and delete access for Operation Technology (OT) extension classes. **Note:** Users assigned the **cmdb_ot_editor** role can edit and delete only OT configuration items (CIs), but they aren't permitted to edit IT CIs.
Operational Technology Manager Admin [cmdb_ot_admin]	Create, read, update, and delete access for Operational Technology (OT) device records. Can also edit and manage specific configurations in the OT entity type. To learn more, see Operation Technology (OT) extension classes. **Note:** Users assigned the **cmdb_ot_admin** role can edit and delete only OT configuration items (CIs), but they aren't permitted to edit IT CIs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Script includes installed with Operational Technology Manager

The Operational Technology Manager plugin installs the following script includes.

Name	Description
BaseDAO	Base DAO class that all DAO classes should extend.
NIDSUtils	Utilities for the cmdb_ci_nids devices.
OTDevicesMigrationUtils	Migrate records from specified classes to updated class tables. For more information, see Operational Technology (OT) extension classes.
OTDevice	Implementation class for performing operations on the [cmdb_ot_entity] table and related [cmdb_ci] and [cmdb_rel_ci] tables.
OTDeviceDAO	Utilities to assist with using IT Discovery for Operational Technology (OT) Network devices.
OTBaseDAO	Base DAO class that all DAO classes in OT should extend.
OTFoundationConstants	A collection of constants used by other script includes.
OTUtils	A collection of OT utility methods.
SGOTDeviceConstants	A collection of constants used by OT Service Graph Connectors.
SGOTDeviceTransformUtil	A collection of transform utility methods for OT Service Graph Connectors.
SGOTDataStreamBase	Base pattern to invoke a specific data stream with given inputs.
SGOTTroubleShootHelper	Helper methods for validating the Service Graph Connector configurations.
OTAssetFilterAjax	A utility client script to filter out application records and OT `Control` Modules from the All OT Devices list view in the Industrial Workspace.
OTBulkEditHandler	Server side script to handle the IT to OT bulk edit (contextualization) and the OT device

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	details bulk edit that are triggered through the Flow Actions and scheduled jobs.
Extension Points	
SGOTDeviceImportExtensionPoint	SG OT Device Import Extension Point which includes two methods: 1. getDeviceCMDBClassNameWithSysId; 2. getComputerType.

Operational Technology Manager Integrations

The Operational Technology Manager application includes support for third-party integrations.

The following third-party integrations are currently supported.

- Service Graph Connector Integration for Claroty CTD
- Service Graph Connector for Microsoft Defender for IoT (Azure)
- Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

Service Graph Connector Integration for Claroty CTD

Integrate Claroty Continuous Threat Detection (CTD) with the ServiceNow Operational Technology Manager application to import detected devices and Claroty CTD sites (sensor or Network Intrusion Detection System appliances).

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Supported versions

Claroty CTD Version:

- 4.4.3 or later
- 5.1

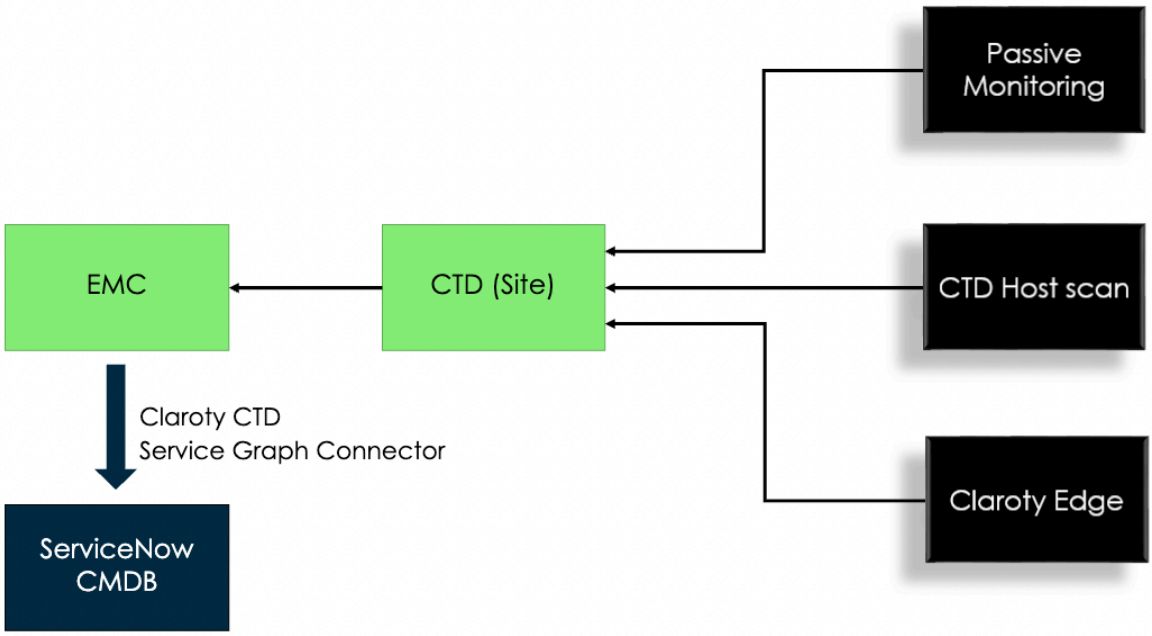
Use cases

Use the Service Graph Connector Integration for Claroty Continuous Threat Detection with the Operational Technology Manager application to import the following information to the Configuration Management Database (CMDB)

- Sites
- Devices detected by each site
- Connections (or baselines)
- Installed programs

The following figure shows the detection method for importing Claroty CTD data into the CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Guided setup

The guided setup for the Service Graph Connector Integration for Claroty CTD provides an organized sequence of tasks to configure the integration on your instance. To access the guided setup, see Configure guided setup.

CMDB integrations dashboard

The Integration Commons for CMDB store app provides a dashboard with a central view of the status, processing results, and processing errors of all installed integrations. You can see metrics for all integration runs. You can filter the view to a specific CMDB integration, a specific time duration, or a specific integration run. For more details about monitoring integrations in the CMDB Integrations Dashboard, see Integration Commons for CMDB.

Data mapping

Data from the Claroty CTD data sources is mapped and transformed into the ServiceNow CMDB Configuration Item (CI) class definitions using the Robust Transform Engine (RTE). Data is inserted into the ServiceNow CMDB using the Identification and Reconciliation Engine (IRE).

The following table lists the data sources included for the Service Graph Connector Integration for Claroty CTD and the corresponding staging tables where the imported data is loaded.

Data sources and staging tables for Claroty CTD

Data source	Staging table
SG-OT Claroty CTD Devices	SG-OT Claroty CTD Devices Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_devices_import]
SG-OT Claroty CTD Baselines	SG-OT Claroty CTD Baselines Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_baselines_import]
SG-OT Claroty CTD Programs	SG-OT Claroty CTD Programs Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_programs_import]
SG-OT Claroty CTD Sites	SG-OT Claroty CTD Sites Import [sn_clarotyctdsgc_sg_ot_claroty_ctd_sites_import]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The imported data from the staging tables is then inserted into the following target tables:

- Computer [cmdb_ci_computer]
- Hardware [cmdb_ci_hardware]
- IP Address [cmdb_ci_ip_address]
- Network Adapter [cmdb_ci_network_adapter]
- OT Device Details [cmdb_ot_entity]
- OT Control Module [cmdb_ci_ot_control_module]
- OT Control System [cmdb_ci_ot_control]
- Serial Number [cmdb_serial_number]

For more information, see CMDB classes targeted.

Default query parameters for the Service Graph Connector Integration for Claroty CTD

By default, the Service Graph Connector Integration for Claroty CTD is shipped with query parameter filters. You can modify their values based on ServiceNow entitlements that you have with the IntegrationHub Enterprise package.

When you begin importing the data from the Claroty CTD, the Service Graph Connector Integration for Claroty CTD uses the default query parameter filters that are listed in the following table.

Default query parameter filters

Query parameter filter	Value	Description
approved_exact	true	Unapproved devices on the Claroty CTD aren't imported because the value of approved_exact is set to true.
valid_exact	true	Invalid devices on the Claroty CTD aren't imported because the value of valid_exact is set to true.
special_hint_exact	0	Address types that aren't set to 0 (unicast) on the Claroty CTD aren't imported.
ghost_exact	false	If there's an device on the Claroty CTD that is classified as a ghost, the Service Graph Connector Integration for Claroty CTD doesn't import it because the default value is set to false.

Configure the Service Graph Connector Integration for Claroty CTD

Use the guided setup for Service Graph Connector Integration for Claroty CTD to lead you through the integration steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Dependencies and requirements:

- The Integration Commons for CMDB store app, which is automatically installed.
- The CMDB CI Class Models app, which is automatically installed.
- The ITOM Discovery License plugin (com.snc.itom.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.itom.license). For more information, see Request Discovery.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.
- Review that **View** access is enabled in Claroty CTD for the following user permissions to collect data from Claroty CTD to ServiceNow:
  - Visibility
  - Investigation
- The Industrial Core plugin. You must activate this plugin.

  The Industrial Core plugin is required to access the class mappings table for the Service Graph Connector Integration for Claroty CTD. For more information about the Industrial Core plugin, see Industrial Core plugin.

Role required: admin

Note: If you have an earlier version of the Service Graph Connector Integration for Claroty CTD, then don't migrate data from the old connector. You must uninstall the previous version and run the new integration.

Procedure

1. Ensure that the application is set to Service Graph Connector Integration for Claroty CTD by using the application picker.
   For more information, see Application picker.
2. Navigate to **All** > **Service Graph Connector Claroty CTD** > **Guided Setup**.
3. On the Getting started page, select **Get Started**.
4. To configure a MID Server, complete the following:
   a. In the Setup Connections and Credentials section, select the Configure MID server task.
   b. Select **Mark as complete** once you complete the MID Server configuration.
5. To set up the connections records, complete the following:
   a. In the Setup Connections and Credentials section, select the Configure Connections task.
   b. Select **Configure**.
   c. Open the Claroty CTD API record in the Connections table.
   d. In the **Connection URL** field, enter the name of the URL for your Claroty CTD Enterprise Management Console (EMC).
   For example, https://192.168.1.100.
   e. If you're using a MID Server, select the **Use MID Server** check box in the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: If you're not using a MID Server, go to step 5g.

f. From the Advanced MID Server Configuration related list, select a MID Server and a MID Selection.

g. Select **Update**.

h. Repeat steps 5a to 5h to update the **Claroty CTD EMC Base Auth** record.

6. To set up the credentials records, complete the following:
   a. In the Setup Connections and Credentials section, select the Configure Credentials task.
   b. Select **Configure**.
   c. Open the Claroty CTD EMC Base Auth record in the Credentials table.
   d. In the **User name** field, enter the user name that you used to log in to the Claroty CTD EMC.
   e. In the **Password** field, enter the password that you used to log in to the Claroty CTD EMC.
   f. Select **Update**.
7. To test the connection, complete the following:
   a. In the Setup Connections and Credentials section, select the Test/Validate Connection task.
   b. Select the **Test Connection** UI action from the related links section on the data source record for sensors.
   After completing the connection test, view the results. You must perform the suggested troubleshooting steps until the test result returns **Success**.
   c. Check that the connection manager has a valid certificate.

   A valid certificate must be installed for a production environment. For a non-production or proof of concept (POC) instance, you can configure the system properties to enable the integration to work when the connection manager doesn't have a valid certificate. The following table lists the system properties that you can configure for a non-production environment.

System properties for a non-production environment

Property	Value
com.glide.communications.httpclient.verify_hostname	Set to **false**.
com.glide.communications.httpclient.verify_revoked_certificate	Set to **false**. If you need to add this system property, see Add a system property.
com.glide.communications.trustmanager_trustall	Set to **true**.

   d. Check the MID security policy.
   In the intranet record, verify that the columns in the following table show the specified values.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Intranet record values

Column	Value
Certificate chain check	**false**
Hostname check	**false**
Revocation check	**false**

For more information, see MID Server certificate check policies.

8. To set the system properties that configure the API resource paths, pagination sizes, and API key expiration times,complete the following:

   a. In the Configure System Properties section, select **Configure**.

   b. Configure the system properties in the following table:

Property	Description
sn_clarotyctdsgc.resourcepath.site	Property to set the resource path for the sites: **Note:** The resource path for the sites is provided by default for the Claroty CTD Enterprise Management Console (EMC) V4.4.3 API version for the CTD sites and devices. If you want to use a different API version, you can override the paths.
sn_clarotyctdsgc.resourcepath.device	Property to set the resource path for the devices: **Note:** The resource path for the devices is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices. If you want to use a different API version, you can override the paths.
sn_clarotyctdsgc.pagesize.device	Property to set the number of device records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page. **Note:** 500 is the maximum number of devices per page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
sn_clarotyctdsgc.resourcepath.baseline	Property to set the resource path for the baselines: **Note:** The resource path for the baselines is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices. If you want to use a different API version, you can override the paths.
sn_clarotyctdsgc.pagesize.baseline	Property to set the number of baseline records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page.
sn_clarotyctdsgc.get_all_baselines	Property to fetch all records for baselines or only the new records since the start time of the last successful import. **Note:** When you import baselines for the first time, all records are imported regardless of the setting for this property.
sn_clarotyctdsgc.resourcepath.entity	Property to set the resource path for the entities: **Note:** The resource path for the entities is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices. If you want to use a different API version, you can override the paths.
sn_clarotyctdsgc.resourcepath.program	Property to set the resource path for the installed programs: **Note:** The resource path for the installed programs is provided by default for the CTD EMC V4.4.3 API version for the CTD sites and devices. If you want to use a different API version, you can override the paths.
sn_clarotyctdsgc.pagesize.entity	Property to set the number of entity records to fetch in a paginated REST call to the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
	Claroty CTD EMC. The default value is 500 records per page.
sn_clarotyctdsgc.pagesize.program	Property to set the number of program records to fetch in a paginated REST call to the Claroty CTD EMC. The default value is 500 records per page.
sn_clarotyctdsgc.api_token_life_in_minutes	Property to set the number of minutes that the API is considered active. After the time expires, the Service Graph Connector fetches a new API key during the next import. The default value is 0 and a new token is fetched for each REST call. **Note:** You can change the value to keep the same token for a maximum of 24 hours and reduce the number of REST calls.
sn_clarotyctdsgc.classify_based_on_os	Property to provide a list of classes that support the classification by OS as part of the Service Graph Connector Integration for Claroty CTD. When the flag is set to **True**, the classification by OS is supported. When it is set to **False**, the Service Graph Connector no longer classifies by OS. For example: `{ "cmdb_ci_ip_switch":true, "cmdb_ci_nids":false }`
sn_clarotyctdsgc.filter.asset_type_code	Property to provide a list of codes for device types separated by the delimiter ($). For more information about Claroty types and codes, see CMDB classes targeted. For example, to only import PLC and HMI device types, enter the Claroty type code as 0$1.
sn_clarotyctdsgc.filter.asset_purdue_level	Property to provide a list of Purdue Levels separated by the delimiter ($). For example, to only filter devices with Purdue Levels 1 and 2, To only filter Devices with Purdue Level 1 & 2, set the value as 1 . 0$2 . 0.

c. Select **Save**.

9. To import CTD sites, complete the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In the Configure CTD Sites section, select the Import CTD Sites task.

b. Select **Configure**.

c. Select the **Execute Now** button.

10. To configure Network Intrusion Detection Systems (NIDS), complete the following:

a. In the Configure CTD Sites section, select the Configure NIDS task.

b. Select **Mark as Complete** once you setup the NIDS used to get devices from Claroty CTD.

11. To configure the import schedules to run the sites, devices, baselines, and installed programs, complete the following:

> **Note:** Empty rack slots associated with a PLC are no longer imported into the Configuration Management Database (CMDB).

a. In the Configure Import Schedules section, select the Configure Sites Import Schedule task.

b. Select **Configure**.

c. In the Scheduled Data Imports table, select **SG-OT CTD Sites Scheduled Import**.

- By default, the sites import schedule is configured to run every day at midnight.
- You must import and validate the CTD sites before you import the devices.

d. Complete the following actions as needed to review or change the import schedule as needed:

Action	Description
Enter a conditional script	Enter a conditional script that determines whether a scheduled import should run by selecting **Conditional**.
Change the default import schedule	Change the default import schedule by setting the **Run** field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the **Runs as** field. **Note:** By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see Configure guided setup.
Activate the import	Activate the import by selecting the **Active** check box.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action	Description
Save any schedule changes	Save any schedule changes by selecting **Update**.

e. In the Configure Import Schedules section, select the Configure Devices Import Schedule task.

f. Select **Configure**.

g. In the Scheduled Data Imports table, select **SG-OT CTD Devices Scheduled Import** to review or change the import schedule for your devices.
   - By default, the devices import schedule is configured to run every day at midnight.
   - Devices are queried by the CTD site. The Service Graph Connector only queries for devices that are detected by validated CTD sites.

h. Complete the following actions as needed to review or change the import schedule as needed:

Action	Description
Enter a conditional script	Enter a conditional script that determines whether a scheduled import should run by selecting **Conditional**.
Change the default import schedule	Change the default import schedule by setting the **Run** field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the **Runs as** field. **Note:** By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see Configure guided setup.
Activate the import	Activate the import by selecting the **Active** check box.
Save any schedule changes	Save any schedule changes by selecting **Update**.

i. In the Configure Import Schedules section, select the Configure Baselines Import Schedule task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

j. Select **Configure**.

k. In the Scheduled Data Imports table, select **SG-OT CTD Baselines Scheduled Import** to review or change the import schedule for the baselines.
By default, the baselines import schedule is configured to run after the parent OT Control System runs.

l. Complete the following actions as needed to review or change the import schedule as needed.

Action	Description
Enter a conditional script	Enter a conditional script that determines whether a scheduled import should run by selecting **Conditional**.
Change the default import schedule	Change the default import schedule by setting the **Run** field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the **Runs as** field. **Note:** By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see Configure guided setup.
Activate the import	Activate the import by selecting the **Active** check box.
Save any schedule changes	Save any schedule changes by selecting **Update**.

m. In the Configure Import Schedules section, select the Configure Sites Installed Programs Import Schedule task.

n. Select **Configure**.

o. In the Scheduled Data Imports table, select **SG-OT CTD Installed Programs Scheduled Import** to review or change the schedule for the installed programs import.
By default, the installed programs import schedule is configured to run every day at midnight.

p. Complete the following actions as needed to review or change the import schedule as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action	Description
Enter a conditional script	Change the default import schedule by setting the **Run** field as necessary.
Change the default import schedule	Change the default import schedule by setting the **Run** field as necessary.
Reference a user in the Users table	Reference a user in the Users table by selecting a user in the **Runs as** field. **Note:** By default, this field is set to System Administrator. The selected user must be assigned the admin role for the import to be successful. If left empty, the import schedule uses the roles of the logged-in user.
Run an import	Run an import by selecting Execute Now. You can import either all records or only new records since the start time of the last successful import, based on the system properties configured. For more information, see step 7c.
Activate the import	Activate the import by selecting the **Active** check box.
Save any schedule changes	Save any schedule changes by selecting **Update**.

12. **Optional:** When configuration items (CIs) are created in the CMDB, asset records are created. The asset record contains the model category of the CI. For more information about the model categories for Operational Technology (OT), see Model categories for Operational Technology. To view the model category for an OT device, complete the following:
    a. Navigate to **All** > **Operational Technology (OT)** > **All OT Devices**.
    b. Select an OT device to view its asset record in a new tab.
13. **Optional:** To troubleshoot the Service Graph Connector Integration for Claroty CTD, complete the following:
    a. Select the [OPTIONAL] Troubleshooting the Service Graph Connector for Claroty CTD section.
    b. In the Execute the validations scheduled job task, select **Configure**.
    c. Select **Execute Now**.
    This job performs tasks to validate the configurations for SGC and the connection to Claroty CTD. If configuration issues are found, the validation results report the problem and suggest troubleshooting steps. Wait for the scheduled job to finish.
    d. Once the scheduled job is complete, navigate back to the [OPTIONAL] Troubleshooting the Service Graph Connector for Claroty CTD section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. In the Review validation results task, select **Configure**.
This step opens the execution logs and suggestions of the last troubleshooting run for you to view.

f. Address the suggestions as needed.

Note: You can use the scheduled script at any point after the initial configuration of the Service Graph Connector Integration for Claroty CTD. To trigger validations, navigate to **All** > **Service Graph Connector for Claroty CTD** > **Troubleshooting** > **Run Troubleshooting**. To view the validation results, navigate to **All** > **Service Graph Connector for Claroty CTD** > **Troubleshooting** > **Results**.

For additional information about troubleshooting issues while using the Service Graph Connector Integration for Claroty CTD, see Troubleshooting scenarios for the Service Graph Connector Integration for Claroty CTD (KB1502041).

Validate NIDS sensors

Validate the Network IDS (NIDS) sensors once they're imported to prepare for device import. The sensors can only pass the validation if they aren't in learning mode as such sensors aren't eligible for device import.

Before you begin

It's recommended that you have the CSDM plugin installed. The Service Graph Connector aligns with the life cycle data models as per the CMDB standards. For more information, see Implementing the CSDM framework in stages.

Role required: cmdb_nids_admin

About this task

The **Life Cycle Stage** and **Life Cycle Stage Status** fields are used to capture the learning mode of a sensor. If the Life Cycle Stage field is set to **Operational** and Life Cycle Stage Status is set to **Learning Mode**, then validation is unsuccessful. If the Life Cycle Stage Status field is set to **In Use**, the validation is successful.

Procedure

1. Navigate to **All** > **Network IDS Appliances (NIDS)** > **Sensors**.
2. Select the sensor record that you want to validate.
3. In the NIDS Assigned Meta Data section, add values for the sensor that you want to be assigned to the detected devices.
4. In the NIDS Admin Configuration section, make sure that the **Life Cycle Stage Status** field value isn't **Learning Mode**.
Otherwise, the validation fails.
5. Make sure that the **NIDS network type** field is set based on the NIDS network location.
For example, you can select an NIDS network type of **IT** for a data center deployment of the NIDS, or an NIDS network type of **OT** for an industrial deployment on an Industrial/OT network.

   If you select OT, the OT device details are created for all devices.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. When the attributes are correctly filled out, select **Validate**.

Note:

NOTE: The attributes passed from the sensor to the devices are defined in the sn_cmdb_ci_class.nids_map_fields system property. The following list is the default list of attributes.

- assigned_to
- location
- company
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- zone
- isa_entity_site (only available if you have the Industrial Process Manager application installed)

Accessing the connection details of the Service Graph Connector Integration for Claroty CTD

You can access the connection details of the Service Graph Connector Integration for Claroty CTD in a single view using the common connection framework (CCF) included within the Integration Commons for CMDB (sn_cmdb_int_util) store app.

With the CCF, you can access all the connections used by the Service Graph Connector Integration for Claroty CTD. The connection details include the connection alias, connection properties, data sources, and scheduled data imports associated with a connection. You can also test the connection. For more information, see Accessing the connection details of Service Graph Connectors.

Access the details of a Claroty CTD connection

Access the details of a Claroty CTD connection configured for the Service Graph Connector Integration for Claroty CTD.

Before you begin

Role required: admin

About this task

There are application modules available to navigate to the data sources, system properties, and scheduled data imports for the Service Graph Connector Integration for Claroty CTD separately. However, the common connection framework (CCF) makes it possible to gather all the related data sources and scheduled data imports created for Claroty CTD in one place. You can also test the connection to the source (Claroty CTD) using the related links section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Ensure that the application scope is set to the **Service Graph Connector Integration for Claroty CTD** application by using the application picker.
2. Navigate to **All** > **Service Graph Connector for Claroty CTD** > **Claroty CTD SGC Connection**.
3. On the Service Graph Connections page, select **SG-OT Claroty CTD Default Connection**.
4. **Optional:** To access the system properties, select the **Service Graph Connection Properties** tab.
5. **Optional:** To access the data sources, select the **Service Graph Connection Data Sources** tab.
6. **Optional:** To access the scheduled data imports, select the **Service Graph Connection Scheduled Data Imports** tab.
7. **Optional:** To test your connection with the Claroty CTD platform, select the **Test Connection** related link.
   You can test your connection at any time. When the connection test is complete, you can find the status and suggestions for troubleshooting the failed steps under **Status** and **Suggestion** on the same page respectively.

CMDB classes targeted in the Service Graph Connector Integration for Claroty CTD

When you complete the setup tasks, you can configure the integration periodically to pull data from Claroty CTD. The data is saved in tables that extend from the Configuration item [cmdb_ci] table.

Viewing class mappings

You can view the available class mappings for the Service Graph Connector Integration for Claroty CTD by navigating to **All** > **Service Graph Connector Claroty CTD** > **Class Mappings**. In the class mappings table, you can view the following attributes.

Class mapping attributes

Field	Description
Source Class	The class of the source CI.
Target CMDB class	The expected ServiceNow class for the CI.
OT Device type	The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example: An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is **server** and its device type is **HMI**. **Note:** In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select **No OT Function**. For OT devices where the device type is unknown, select **Unknown**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Class mapping attributes (continued)

Field	Description
Allow OS classification	When set to **True**, if an operating system is found on the CI, the target is switched away from the target CMDB class to a ServiceNow class that matches its OS.
Active	When checked, the class mapping is set to **Active**.

The Service Graph Connector Integration for Claroty CTD also uses Claroty types and codes. For more information, see the Default class mapping table.

Computer [cmdb_ci_computer]

The following attributes in the Computer [cmdb_ci_computer] table are populated by collected data:

Attribute label	Attribute name
Most recent discovery	last_discovered
Operating System	os
OS Version	os_version

External system metadata [cmdb_key_value_v2]

The following attributes in the External system metadata [cmdb_key_value_v2] table are populated by collected data:

Attribute label	Attribute name
Discovery source	discovery_source
Key	key
Source key	source_key
URL value	url_value
Value type	value_type

Firmware Installation [cmdb_firmware_install]

The following attributes in the Firmware Installation [cmdb_firmware_install] table are populated by collected data:

Attribute label	Attribute name
Source Native Key	firmware_version_snk
IRE criterion attribute	firmware_ire_criterion_key
Discovered version	firmware_version_cleansed
Discovery source	firmware_version_discovery_source

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware [cmdb_ci_hardware]

The following attributes in the Hardware [cmdb_ci_hardware] table are populated by collected data:

Attribute label	Attribute name
Change Group	assignment_group
Support group	support_group
Company	company
Vendor	vendor
Name	name
Serial number	serial_number
Class	sys_class_name
First discovered	first_discovered
Location	location
Model number	model_number
Most recent discovery	last_discovered
Supported by	supported_by
Assigned to	assigned_to
Managed By Group	managed_by_group
Managed by	managed_by
Model ID	model_id
Approval group	change_control
Owned by	owned_by
Manufacturer	manufacturer

Relationships created for Hardware

Parent class	Relationship type	Child class
Hardware [cmdb_ci_hardware]	Owns::Owned by	Network Adapter [cmdb_ci_network_adapter]
Hardware [cmdb_ci_hardware]	Owns::Owned by	IP Address [cmdb_ci_ip_address]
Hardware [cmdb_ci_hardware]	Reference	OT Device [cmdb_ot_entity]
Hardware [cmdb_ci_hardware]	Reference	External system metadata [cmdb_key_value_v2]
Hardware [cmdb_ci_hardware]	Reference	Software Installation [cmdb_sam_sw_install]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IP Address [cmdb_ci_ip_address]

The following attributes in the IP Address [cmdb_ci_ip_address] table are populated by collected data:

Attribute label	Attribute name
Owned By Configuration Item	owned_by_cmdb_ci
IP Address	ip_address
IP version	ip_version

Relationships created for IP Address

Parent class	Relationship type	Child class
IP Address [cmdb_ci_ip_address]		Network Intrusion Detection System [cmdb_ci_nids]
IP Address [cmdb_ci_ip_address]		Hardware [cmdb_ci_hardware]

Network Adapter [cmdb_ci_network_adapter]

The following attributes in the Network Adapter [cmdb_ci_network_adapter] table are populated by collected data:

Attribute label	Attribute name
MAC Address	mac_address
Name	name

Relationships created for Network Adapter

Parent class	Relationship type	Child class
Network Adapter [cmdb_ci_network_adapter]	Reference	Hardware [cmdb_ci_hardware]

Network Intrusion Detection System [cmdb_ci_nids]

The following attributes in the Network Intrusion Detection System [cmdb_ci_nids] table are populated by collected data:

Attribute label	Attribute name
Manufacturer	manufacturer
Name	name
Correlation ID	correlation_id
Description	short_description
Firmware version	firmware_version

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute label	Attribute name
NIDS manager connection state	connection_state
Life Cycle Stage Status	life_cycle_stage_status
Life Cycle Stage	life_cycle_stage
Validated	validated

Relationships created for NIDS

Parent class	Relationship type	Child class
Network Intrusion Detection System [cmdb_ci_nids]	Owns::Owned by	IP Address [cmdb_ci_ip_address]
Network Intrusion Detection System [cmdb_ci_nids]	Detects::Detected by	Hardware [cmdb_ci_hardware]

Operational Technology (OT) [cmdb_ci_ot]

The following attributes in the Operational Technology (OT) [cmdb_ci_ot] table are populated by collected data:

Attribute label	Attribute name\
Firmware version	firmware_version
Most recent discovery	last_discovered

OT Device [cmdb_ot_entity]

The following attributes in the OT Device [cmdb_ot_entity] table are populated by collected data:

Attribute label	Attribute name
Purdue level	purdue_level
ISA entity site	isa_entity_site
OT discovery source ID	ot_correlation_id
Device criticality	business_criticality
Zone	zone
OT device type	ot_asset_type
IRE criterion attribute	ire_criterion_attribute

OT Control Module [cmdb_ci_ot_control_module]

The following attributes in the OT Control Module [cmdb_ci_ot_control_module] table are populated by collected data:

Attribute label	Attribute name
Location	location

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute label	Attribute name
Supported by	supported_by
Name	name
Serial number	serial_number
Slot number	slot_number
Manufacturer	manufacturer
Firmware version	firmware_version
Approval group	change_control
Assigned to	assigned_to
Most recent discovery	last_discovered
Model ID	model_id
Model number	model_number
Company	company
Owned by	owned_by
Managed by	managed_by
Support group	support_group
Managed By Group	managed_by_group
Change Group	assignment_group
Vendor	vendor

Relationships created for OT Control Module

Parent class	Relationship type	Child class
OT Control Module [cmdb_ci_ot_control_module]	Reference	OT Device [cmdb_ot_entity]

OT Control System [cmdb_ci_ot_control]

The following attributes in the OT Control System [cmdb_ci_ot_control] table are populated by collected data:

Attribute label	Attribute name
Has module	has_module
Most recent discovery	last_discovered

Relationships created for OT Control System

Parent class	Relationship type	Child class
OT Control System [cmdb_ci_ot_control]	Owns::Owned by	OT Control Module [cmdb_ci_ot_control_module]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Serial Number [cmdb_serial_number]

The following attributes in the Serial Number [cmdb_serial_number] table are populated by collected data:

Note: A fix script is automatically applied to clean up the serial number [cmdb_serial_number] records imported into the sys_object_source table from the Service Graph Connector. The script ensures that a null pointer exception doesn't occur when a serial number and MAC address are the same.

This fix script only runs once during the upgrade of Service Graph Connector Integration for Claroty CTD but doesn't run on zbooted instances or fresh installation. This doesn't affect the functionality or lead to any data loss.

Attribute label	Attribute name
Serial Number	serial_number
Serial Number Type	serial_number_type
Valid	valid

Relationships created for Serial Number

Parent class	Relationship type	Child class
Serial Number [cmdb_serial_number]	Reference	Hardware [cmdb_ci_hardware]

Software [cmdb_ci_spkg]

The following attributes in the Software [cmdb_ci_spkg] table are populated by collected data:

Attribute label	Attribute name
Key	key
Version	version
Manufacturer	manufacturer
Name	name

Relationships created for Software

Parent class	Relationship type	Child class
Software [cmdb_ci_spkg]	Reference	Software Instance [cmdb_software_instance]

Software Instance [cmdb_software_instance]

The following attributes in the Software Instance [cmdb_software_instance] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Attribute label	Attribute name
Install date	install_date
Installed on	installed_on
Name	name

Relationships created for Software Instance

Parent class	Relationship type	Child class
Software Instance [cmdb_software_instance]	Reference	Hardware [cmdb_ci_hardware]

Software Installation [cmdb_sam_sw_install]

The following attributes in the Software Installation [cmdb_sam_sw_install] table are populated by collected data:

Attribute label	Attribute name
Display name	display_name
Version	version
Discovery source	discovery_source

Relationships created for Software Installation

Parent class	Relationship type	Child class
Software Instance [cmdb_software_instance]	Reference	Hardware [cmdb_ci_hardware]

Default class mapping

A default class mapping is shipped with the Service Graph Connector Integration for Claroty CTD application.

Note: You can find the class mapping in the **sn_clarotyctdsgc.SGOTClarotyCTDConstants** script.

Claroty CTD Type	ServiceNow Type	Class	OT Entity Type	Claroty Types and Codes
eAAAServer	(Empty)	cmdb_ci_server		eAAAServer = 61
eAccessControl	(Empty)	cmdb_ci_iot		eAccessControl = 50
eAccessPoint	(Empty)	cmdb_ci_ip_switch		eAccessPoint = 60
eADServer	(Empty)	cmdb_ci_server		eADServer = 33

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Claroty CTD Type	ServiceNow Type	Class	OT Entity Type	Claroty Types and Codes
eAutonomousVehicle	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eAutonomousVehicle = 58
eAVServer	(Empty)	cmdb_ci_server		eAVServer = 32
eBarcodeScanner	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eBarcodeScanner = 48
eBluetoothDevice	(Empty)	cmdb_ci_iot		eBluetoothDevice = 41
eBroadcast	(Empty)	cmdb_ci_netgear		eBroadcast = 4
eCamera	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eCamera = 42
eCleaningDevice	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eCleaningDevice = 55
eController	OT Control System	cmdb_ci_ot_control	ot_control_system	eController = 20
eDataLogger	OT Control System	cmdb_ci_ot_control	ot_control_system	eDataLogger = 66
eDBServer	(Empty)	cmdb_ci_server		eDBServer = 35
eDomainController	(Empty)	cmdb_ci_server		eDomainController = 5
eElectricalDrive	Industrial Drive	cmdb_ci_ot_industrial_drive	industrial_drive	eElectricalDrive = 68
eEndpoint	Operational Technology Device	cmdb_ci_ot	ot_base	eEndpoint = 2
eEngineeringStation	EWS	cmdb_ci_ot_ews	ews	eEngineeringStation = 14
eFileServer	(Empty)	cmdb_ci_server		eFileServer = 10
eFirewall	(Empty)	cmdb_ci_ip_firewall		eFirewall = 31
eFrontEndProcessor	OT Control System	cmdb_ci_ot_control	ot_control_system	eFrontEndProcessor = 26
eGateway	(Empty)	cmdb_ci_ip_switch		eGateway = 15
eGPSClock	Operational Technology Device	cmdb_ci_ot	ot_base	eGPSClock = 37
eGPSDevice	Operational Technology Device	cmdb_ci_ot	ot_base	eGPSDevice = 62
eHistorian	Historian	cmdb_ci_ot_historian	historian	eHistorian = 9
eHMI	HMI	cmdb_ci_ot_hmi	hmi	eHMI = 1
eHomeAssistant	(Empty)	cmdb_ci_iot		eHomeAssistant = 53
eIED	IED	cmdb_ci_ot_ied	ied	eIED = 19

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Claroty CTD Type	ServiceNow Type	Class	OT Entity Type	Claroty Types and Codes
eInfusionPump	(Empty)	cmdb_ci_iot		eInfusionPump = 46
eMediaServer	(Empty)	cmdb_ci_server		eMediaServer = 54
eMedicalDevice	(Empty)	cmdb_ci_iot		eMedicalDevice = 47
eMicroscope	(Empty)	cmdb_ci_iot		eMicroscope = 49
eModem	(Empty)	cmdb_ci_netgear		eModem = 27
eMotorStarter	Industrial Drive	cmdb_ci_ot_industrial_drive	industrial_drive	eMotorStarter = 69
eNetworkAccessStorage	(Empty)	cmdb_ci_server		eNetworkAccessStorage = 30
eNetworking	(Empty)	cmdb_ci_netgear		eNetworking = 3
eNTPServer	(Empty)	cmdb_ci_server		eNTPServer = 21
eOPCServer	OPC Server	cmdb_ci_ot_opc_server	opc_server	eOPCServer = 16
eOT	Operational Technology Device	cmdb_ci_ot	ot_base	eOT = 17
ePLC	PLC	cmdb_ci_ot_plc	plc	ePLC = 0
ePrinter	(Empty)	cmdb_ci_printer		ePrinter = 6
eProxyServer	(Empty)	cmdb_ci_netgear		eProxyServer = 28
eRemoteIO	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eRemoteIO = 13
eReverseProxyServer	(Empty)	cmdb_ci_netgear		eReverseProxyServer = 29
eRobot	Industrial Robot	cmdb_ci_ot_industrial_robot	industrial_robot	eRobot = 57
eRouter	Router	cmdb_ci_ip_router		eRouter = 11
eRTU	RTU	cmdb_ci_ot_rtu	rtu	eRTU = 18
eSCADAClient	SCADA Client	cmdb_ci_ot_scada_client	scada_client	eSCADAClient = 7
eSCADAMaster	SCADA Server	cmdb_ci_ot_scada_server	scada_server	eSCADAMaster = 38
eSCADAServer	SCADA Server	cmdb_ci_ot_scada_server	scada_server	eSCADAServer = 8
eSensor	Industrial Sensor	cmdb_ci_ot_industrial_sensor	industrial_sensor	eSensor = 67
eSmartLight	(Empty)	cmdb_ci_iot		eSmartLight = 51
eSmartPhone	(Empty)	cmdb_ci_iot		eSmartPhone = 44

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Claroty CTD Type	ServiceNow Type	Class	OT Entity Type	Claroty Types and Codes
eSmartWatch	(Empty)	cmdb_ci_iot		eSmartWatch = 45
eStorageArray	(Empty)	cmdb_ci_server		eStorageArray = 36
eStreamer	(Empty)	cmdb_ci_iot		eStreamer = 52
eSwitch	(Empty)	cmdb_ci_ip_switch		eSwitch = 12
eSyslogServer	(Empty)	cmdb_ci_server		eSyslogServer = 25
eTerminalServer	(Empty)	cmdb_ci_server		eTerminalServer = 24
eTVScreen	(Empty)	cmdb_ci_iot		eTVScreen = 40
eUPS	(Empty)	cmdb_ci_ups		eUPS = 63
eUserConsole	HMI	cmdb_ci_ot_hmi	hmi	eUserConsole = 22
eUserWorkstation	HMI	cmdb_ci_ot_hmi	hmi	eUserWorkstation = 23
eVendingMachine	(Empty)	cmdb_ci_iot		eVendingMachine = 43
eVideoRecorder	(Empty)	cmdb_ci_server		eVideoRecorder = 64
eVirtualizationServer	(Empty)	cmdb_ci_server		eVirtualizationServer = 65
eVoipPhone	(Empty)	cmdb_ci_comm_hardware		eVoipPhone = 39
eVoipServer	(Empty)	cmdb_ci_server		eVoipServer = 56
eWebServer	(Empty)	cmdb_ci_server		eWebServer = 34
eWirelessLanController	(Empty)	cmdb_ci_netgear		eWirelessLanController = 59
eBarcodeReader	(Empty)	cmdb_ci_iot		eBarcodeReader = 77
eBiometricScanner	(Empty)	cmdb_ci_iot		eBiometricScanner = 74
eDNSServer	(Empty)	cmdb_ci_server		eDNSServer = 75
eSNMPScanner	(Empty)	cmdb_ci_server		eSNMPScanner = 73
eSNMPServer	(Empty)	cmdb_ci_server		eSNMPServer = 72
eVisionCamera	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eVisionCamera = 76
eVisionController	OT Control System	cmdb_ci_ot_control	ot_control_system	eVisionController = 78

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Claroty CTD Type	ServiceNow Type	Class	OT Entity Type	Claroty Types and Codes
eVisionSensor	OT Field Device	cmdb_ci_ot_field_device	ot_field_device	eVisionSensor = 79
eVOIPAccessPoint	(Empty)	cmdb_ci_ip_switch		eVOIPAccessPoint = 71
eVulnerabilityScanner	(Empty)	cmdb_ci_server		eVulnerabilityScanner = 70

Service Graph Connector for Microsoft Defender for IoT (Azure)

Integrate Microsoft Defender for IoT with the ServiceNow® Operational Technology Manager application to automate import of OT devices and sensor appliances.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Supported versions

Supports Microsoft Defender for IoT sensor versions:

- 22.2.3.22
- 22.2.5.9

Use cases

You can use the Service Graph Connector for Microsoft Defender for IoT (Azure) with the ServiceNow® Operational Technology Manager application to import OT devices and sensor appliances.

Guided setup

The guided setup for the Service Graph Connector for Microsoft Defender for IoT (Azure) provides an organized sequence of tasks to configure the integration on your instance. To access the guided setup, see Configure guided setup.

CMDB integrations dashboard

The Integration Commons for CMDB store app provides a dashboard with a central view of the status, processing results, and processing errors of all installed integrations. You can see metrics for all integration runs. You can filter the view to a specific CMDB integration, a specific time duration, or a specific integration run. For more details about monitoring integrations in the CMDB Integrations Dashboard, see Integration Commons for CMDB.

Data mapping

Data from the Microsoft Defender for IoT (Azure) data sources is mapped and transformed into the ServiceNow CMDB Configuration Item (CI) class definitions using the Robust Transform Engine (RTE). Data is inserted into the ServiceNow CMDB using the Identification and Reconciliation Engine (IRE).

When you complete the setup, you can configure the integration to periodically pull data from the Microsoft Defender for IoT (Azure) application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following table lists the data sources included for a Microsoft Defender for IoT (Azure) project and the corresponding staging tables where the imported data is loaded.

Data sources and staging tables for Microsoft Defender for IoT (Azure)

Data source	Staging table
SG-OT Azure D4IoT Devices Import	SG-OT Azure D4IoT Devices Import [sn_msftd4iotazsgc_sg_ot_azure_d4iot_devices_import]
SG-OT Azure D4IoT Sensors Import	SG-OT Msft D4IoT Sensors Import [sn_msftd4iotazsgc_sg_ot_azure_d4iot_sensors_import]

The imported data from the staging tables is then inserted into the following target tables:

- AIX Server [cmdb_ci_aix_server]
- Computer [cmdb_ci_computer]
- Configuration Item [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX Server [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- External System Metadata [cmdb_key_value_v2]
- Game Console [cmdb_ci_game_console]
- Handheld Computing Device [cmdb_ci_handheld_computing]
- Historian [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX Server [cmdb_ci_hpux_server]
- HVAC Equipment [cmdb_ci_hvac]
- HyperV Server [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- Industrial Actuator [cmdb_ci_ot_industrial_actuator]
- Industrial Drive [cmdb_ci_ot_industrial_drive]
- Industrial Robot [cmdb_ci_ot_industrial_robot]
- Industrial Sensor [cmdb_ci_ot_industrial_sensor]
- IoT Device [cmdb_ci_iot]
- IP Address [cmdb_ci_ip_address]
- IP Camera [cmdb_ci_ip_camera]
- IP Firewall [cmdb_ci_ip_firewall]
- IP Phone [cmdb_ci_ip_phone]
- Linux Server [cmdb_ci_linux_server]
- Netgear [cmdb_ci_netgear]
- Network Adapter [cmdb_ci_network_adapter]
- Network Intrusion Detection System [cmdb_ci_nids]
- Operational Technology (OT) [cmdb_ci_ot]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- OSX Server [cmdb_ci_osx_server]
- OT Control Module [cmdb_ci_ot_control_module]
- OT Control System [cmdb_ci_ot_control]
- OT Device Details [cmdb_ot_entity]
- OT Field Device [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- Printer [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- Serial Number [cmdb_serial_number]
- Server [cmdb_ci_server]
- Server [cmdb_ci_server]
- Solaris Server [cmdb_ci_solaris_server]
- Source [sys_object_source]
- Unix Servercmdb_ci_unix_server]
- Uninterruptible Power Supply (UPS) [cmdb_ci_ups]
- Wireless Access Point [cmdb_ci_wap_network]

For more information on where data is saved when pulling data from a Microsoft Defender for IoT (Azure) project, see CMDB classes targeted.

Configure the Service Graph Connector for Microsoft Defender for IoT (Azure)

Use the guided setup for the Service Graph Connector for Microsoft Defender for IoT (Azure) to lead you through the integration steps.

Before you begin

Dependencies and requirements:

- The Integration Commons for CMDB store app, which is automatically installed.
- The CMDB CI Class Models app, which is automatically installed.
- The ITOM Discovery License plugin (com.snc.itom.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.itom.license). For more information, see Request Discovery.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.
- The Industrial Core plugin. You must activate this plugin.

  The Industrial Core plugin is required to access the class mappings table for the Service Graph Connector for Microsoft Defender for IoT (Azure). For more information about the Industrial Core plugin, see Industrial Core plugin.

Role required: admin

Note: If you have an earlier version of the Service Graph Connector for Microsoft Defender for IoT (Azure), then don't migrate data from the old connector. You must uninstall the previous version and run the new integration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Ensure that the application scope is set to the Service Graph Connector for Microsoft Defender for IoT (Azure) application by using the application picker.
   For more information, see Application picker.
2. Navigate to **All** > **Service Graph for MSFT D4IoT (Azure)** > **Guided Setup**.
3. On the Getting started page, select **Get Started**.
4. To access the Azure resources, complete the following:
   a. Select the Access to Azure Resources task.
   b. Once you complete the instructions in the description, select **Mark as Complete**.
5. To set up the connections and credentials, complete the following:
   a. In the Configure Connections and Credentials section, select the Setup Connections and Credentials task.
   b. Select **Configure**.
   c. Select the **SG-OT Azure Connection** record.
   d. Select the Create New Connection & Credential related link.
   e. In the Create Connection and Credential window, fill in the following fields.

Field	Description
Connection Name	Display name for the connection record
Connection URL	Azure URL
OAuth Client ID	Client ID (application ID) or Service Principal ID
OAuth Client Secret	Client secret key associated with the Service Principal
OAuth Token URL	URL to fetch Authorization token. Replace <tenantid> in the URL with the Tenant ID value.

   Note: When a token generation is successful, a new window appears with a success message. When a token generation isn't successful, a new window with the error message `OAuth flow failed` appears. Please check the details provided and try again by editing the record you created.

   f. Select **Create and Get OAuth Token**.
6. To test the connection, complete the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. In the Setup Connections and Credentials section, select the Test/Validate Connection task.

b. Select the **Test Connection** UI action from the related links section on the data source record for sensors.
After completing the connection test, view the results. You must perform the suggested troubleshooting steps until the test result returns **Success**.

7. To configure the system properties, complete the following:

a. In the Configure System Properties section, select **Configure**.

b. Configure the following system properties.

Property	Description
sn_msftd4iotazsgc.resource_path	Set the resource path property. The default Resource Path for the ARG REST API version 2021-03-01 is `/providers/Microsoft.ResourceGraph/resources`.
sn_msftd4iotazsgc.pagesize.sensor	Set the page size property for sensors. ▪ As Azure ARG REST API supports pagination, you can choose the number of records per page for each API. ▪ The default is 1000 records per page. **Note:** 1000 is also the maximum number of records per page.
sn_msftd4iotazsgc.pagesize.device	Set the page size property for devices. ▪ As Azure ARG REST API supports pagination, you can choose the number of records per page for each API. ▪ The default is 1000 records per page. **Note:** 1000 is also the maximum number of records per page.
sn_msftd4iotazsgc.get_all_devices	▪ For devices, you can choose to fetch all records (box checked) or the delta (box unchecked). ▪ The DELTA fetches all the records created or updated since the start time of the last successful import in the CMDB. **Note:** When you run the Devices Integration for the first time, all records are imported independent of this property.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
sn_msftd4iotazsgc.convert_sensor_names_to_lowercase	Set this property for devices import. ▪ This system property is used to convert the sensor names provided by Microsoft Azure into lowercase while importing devices. ▪ This is required as Microsoft Azure expects data for the query in a lowercase format.
sn_msftd4iotazsgc.filter.device_sub_types	Set this property for filtering the devices during device import by sub type. ▪ Comma-separated list of Microsoft Azure sub types to filter the devices. ▪ For example: to import only PLCs and servers, provide the value from the DeviceSubType attribute from Microsoft Azure as `Server, PLC`.
sn_msftd4iotazsgc.filter.device_tags	Set this property for filtering the devices during device import by device tag. ▪ Comma-separated list of case sensitive tags that are needed to filter devices. ▪ For example: to import devices with specific tags, provide a list of values from the DeviceTags attribute in Microsoft Azure.
sn_msftd4iotazsgc.filter.custom_query	Set this property to add more filters for device import apart from the Device SubType and Device Tags filter. ▪ Query to filter based on other attributes. ▪ This allows filtering for other attributes. For more information, see Azure Query Language.
sn_msftd4iotazsgc.azure_d4iot_site_map_fields	An object of fields from the Microsoft Defender for IoT (Azure) Site Map. When a field is set to **True**, the Service Graph Connector for Microsoft Defender for IoT (Azure) passes the value of the Site Map field to the corresponding field on each CI discovered by the integration at the Azure site. If set to **False** or not populated on the Site Map record, the field isn't set on the imported CIs associated with the Azure site. For consistency with the other integrations using the NIDS framework, check this system property. By default, only **location** and **equipment_model_entity** are set to **True**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
sn_msftd4iotazsgc.devices_fetch_type	Indicates if devices are fetched per sensor, Active Scan devices, or both.
sn_msftd4iotazsgc.active_scan_get_all_devices	Set this system property to import all Active Scan devices. If not checked, then only the Active Scan devices created or updated since the last successful import are imported. The default value is **No**.
sn_msftd4iotazsgc.filter.active_scan.device_subtypes	Comma-separated list of Azure subtypes to filter the Active Scan devices. For example, to only import PLCs and servers, provide the value from the Device SubType attribute as `Server, PLC` in Azure.
sn_msftd4iotazsgc.filter.active_scan.device_tags	Comma-separated list of case sensitive tags needed to filter Active Scan devices. For example, to import Active Scan devices with specific tags, provide a list of values from the DeviceTags attribute from Azure.
sn_msftd4iotazsgc.filter.active_scan.custom_query	Query to filter other attributes for Active Scan devices. For example, to allow filtering on other attributes. For more information about the Azure query language, see Azure Query Language for more information.

c. Select **Save**.

8. To import sensors, complete the following:
   a. In the Configure Sensors (NIDS) section, select the Import Sensors task.
   b. Select **Configure**.
   c. Select **Active** to activate the Scheduled Data Import job.
9. To configure the NIDS, complete the following:
   a. In the Configure Sensors (NIDS) section, select the Import Sensors task.
   b. Select **Mark as complete** once you complete the NIDS configuration linked in the description.
10. To configure import schedules, complete the following:
    a. In the Configure Import Schedules section, select **Configure**.
    b. Select **SG-OT Microsoft Azure D4IoT Sensors Scheduled Import** to review or change the sensors import schedule as needed.
       i. Select **Active** to activate the sensors import schedule.
       ii. By default, the sensors import schedule is configured to run daily at midnight. Change the schedule using the **Run** and **Time** fields.
       iii. Select the **Conditional** check box to make this schedule conditional.
       iv. Select **Execute Now** to start a manual import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Select **SG-OT Microsoft Azure D4IoT Devices Scheduled Import** to review or change the devices import schedule as needed.

i. Select **Active** to activate the sensors import schedule.

ii. By default, the sensors import schedule is configured to run daily at midnight. Change the schedule using the **Run** and **Time** fields.

iii. Select the **Conditional** check box to make this schedule conditional.

iv. Select **Execute Now** to start a manual import.

Note: Devices are queried per sensor. The Service Graph Connector only queries for devices detected by a validated sensor. For more information, see step 9.

11. **Optional:** When configuration items (CIs) are created in the CMDB, asset records are created. The asset record contains the model category of the CI. For more information about the model categories for Operational Technology (OT), see Model categories for Operational Technology. To view the model category for an OT device, complete the following:

a. Navigate to **All** > **Operational Technology (OT)** > **All OT Devices**.

b. Select an OT device to view its asset record in a new tab.

12. **Optional:** To troubleshoot the Service Graph Connector for Microsoft Defender for IoT (Azure), complete the following:

a. Select the [OPTIONAL] Troubleshooting the Service Graph Connector for Microsoft Defender for IoT (Azure) section.

b. In the Execute the validations scheduled job task, select **Configure**.

c. Select **Execute Now**.
This job performs tasks to validate the configurations for SGC and the connection to Microsoft Azure. If configuration issues are found, the validation results report the problem and suggest troubleshooting steps. Wait for the scheduled job to finish.

d. Once the scheduled job is complete, Navigate back to the [OPTIONAL] Troubleshooting the Service Graph Connector for Microsoft Defender for IoT (Azure) section.

e. In the Review validation results task, select **Configure**.
This step opens the execution logs and suggestions of the last troubleshooting run for you to view.

f. Address the suggestions as needed.

Note: You can use the scheduled script at any point after the initial configuration of the Service Graph Connector Integration for Claroty CTD. To trigger validations, navigate to **All** > **Service Graph for MSFT D4IoT (Azure)** > **Troubleshooting** > **Run Troubleshooting**. To view the validation results, navigate to **All** > **Service Graph for MSFT D4IoT (Azure)** > **Troubleshooting** > **Results**.

What to do next

You can now connect Microsoft Defender for IoT (Azure) with the ServiceNow Service Graph Connector for Microsoft Defender for IoT (Azure). For more information, see Connecting your Microsoft Defender for IoT (Azure) subscription to the ServiceNow Service Graph Connector for Microsoft Defender for IoT (Azure) (KB1587770).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Validate NIDS sensors

Validate the Network IDS (NIDS) sensors once they're imported to prepare for the device import. Sensors only pass the validation if they aren't in learning mode as such sensors are not eligible for device import.

Before you begin

It's recommended that you have the CSDM plugin installed. The Service Graph Connector aligns with the life cycle data models as per the CMDB standards. For more information, see Implementing the CSDM framework in stages.

Role required: cmdb_nids_admin

Note: An NIDS appliance in ServiceNow represents a Microsoft Defender for IoT (Azure) sensor.

About this task

The **Life Cycle Stage** and **Life Cycle Stage Status** fields are used to capture the learning mode of a sensor. If the Life Cycle Stage field is set to **Operational** and Life Cycle Stage Status is set to **Learning Mode**, then validation is unsuccessful. If the Life Cycle Stage Status field is set to **In Use**, the validation is successful.

Procedure

1. Navigate to **All** > **Network IDS Appliances (NIDS)** > **Sensors**.
2. Select the sensor record that you want to validate.
3. In the NIDS Assigned Meta Data section, add values for the sensor that you want to be assigned to the detected devices.
4. From the NIDS Admin Configuration section, make sure that the **Life Cycle Stage Status** field value isn't **Learning Mode**.
   Otherwise, the validation fails.
5. Make sure that the **NIDS network type** field is set based on the NIDS network location.
   For example, you can select an NIDS network type of **IT** for a data center deployment of the NIDS, or an NIDS network type of **OT** for an industrial deployment on an Industrial/OT network.

   If you select OT, the OT device details are created for all devices.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. When the attributes are correctly filled out, select **Validate**.

Note:

NOTE: The attributes passed from the sensor to the devices are defined in the sn_cmdb_ci_class.nids_map_fields system property. The following list is the default list of attributes.

- assigned_to
- location
- company
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- zone
- isa_entity_site (only available if you have the Industrial Process Manager application installed)

Accessing the connection details of the Service Graph Connector for Microsoft Defender for IoT (Azure)

You can access the connection details of the Service Graph Connector for Microsoft Defender for IoT (Azure) in a single view using the common connection framework (CCF) included within the Integration Commons for CMDB (sn_cmdb_int_util) store app.

With the CCF, you can access all the connections used by the Service Graph Connector for Microsoft Defender for IoT (Azure). The connection details include the connection alias, connection properties, data sources, and scheduled data imports associated with a connection. You can also test the connection. For more information, see Accessing the connection details of Service Graph Connectors.

Access the details of a Microsoft Defender for IoT (Azure) connection

Access the details of a Microsoft Defender for IoT (Azure) connection configured for the Service Graph Connector Integration for Claroty CTD.

Before you begin

Role required: admin

About this task

There are application modules available to navigate to the data sources, system properties, and scheduled data imports for the Service Graph Connector for Microsoft Defender for IoT (Azure) separately. However, the common connection framework (CCF) makes it possible to gather all the related data sources and scheduled data imports created for Microsoft Defender for IoT (Azure) in one place. You can also test the connection to the source (Microsoft Defender for IoT (Azure)) using the related links section.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Ensure that the application scope is set to the Service Graph Connector for Microsoft Defender for IoT (Azure) application by using the application picker.
2. Navigate to **All** > **Service Graph for MSFT D4IoT (Azure)** > **Azure SGC Connection**.
3. On the Service Graph Connections page, select **SG-OT Azure SGC Default Connection** record.
4. **Optional:** To access the system properties, select the **Service Graph Connection Properties** tab.
5. **Optional:** To access the data sources, select the **Service Graph Connection Data Sources** tab.
6. **Optional:** To access the scheduled data imports, select the **Service Graph Connection Scheduled Data Imports** tab.
7. **Optional:** To test your connection with the Microsoft Azure platform, select the **Test Connection** related link.
   You can test your connection at any time. When the connection test is complete, you can find the status and suggestions for troubleshooting the failed steps under **Status** and **Suggestion** on the same page respectively.

Import OT devices using the Standard mode of discovery

Use the Service Graph Connector for Microsoft Defender for IoT (Azure) to import Operational Technology (OT) devices discovered through the Standard mode of discovery from Microsoft Defender for IoT.

Before you begin

Role required: admin

About this task

Standard mode uses an active search to discover additional information about the identified OT devices to supplement the existing device information. The devices identified during standard mode aren't associated with the passive sensor. To import these devices and assign them to a site, you can use the **Site Mappings** table. The table is populated using an automatic scheduled job. After the scheduled job is executed, the system populates the sites from the Source system in the table.

The **Site Mappings** table allows the admin to perform site mappings between the Microsoft Defender for IoT (Azure) site, where this data resides, and the ServiceNow ISA entity site [cmdb_ci_ot_isa_entity]. When the data is imported through the Service Graph Connector for Microsoft Defender for IoT (Azure), the devices are assigned to the correct site in the ISA entity site [cmdb_ci_ot_isa_entity].

Procedure

1. Navigate to **All** > **Service Graph for MSFT D4IoT (Azure)** > **Site Mappings**.
2. Select **New**.
3. On the form, fill in the following fields.

SG-OT Azure D4IoT Site Map fields

Field	Description
ISA Entity Site	Site name for your ISA Entity site.
Azure D4IoT Site	Site name for your Azure D4IoT site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Location	Location of the Azure D4IoT Site
Approval group	Group that can approve requests related to the site.
Azure D4IoT Site URL	
Assigned to	User that the site is assigned to.
Change group	Group that is assigned change requests related to the site.
Company	Company that runs the site.
Managed by	User that manages the site.
Managed by group	Group that manages the site.
Owned by	User that owns the site.
Support group	Group that is contacted when issues are encountered.
Supported by	User that is contacted when issues are encountered.
Network type	Network type of site. For example, **OT**.
Correlation ID	Unique ID that identifies the correlation on the local system.

4. Select **Submit**.

Result
Once the Site Mappings record is created and you perform the device import, devices are imported through the sensor and active scan. The devices are then assigned to an ISA entity [cmdb_ci_ot_isa_entity] site in ServiceNow.

Note: The metadata information from the site record, such as Assigned to and Owned by, are copied to the imported devices using the Service Graph Connector's system properties. For more information about the system properties for the Service Graph Connector for Microsoft Defender for IoT (Azure), see Configure guided setup.

CMDB classes targeted in the Service Graph Connector for Microsoft Defender for IoT (Azure)

When you complete the guided setup, you can configure the integration to periodically pull data from a Service Graph Connector for Microsoft Defender for IoT (Azure) (Azure) project. The data is saved in tables that extend from the Configuration item [cmdb_ci] table.

Viewing class mappings

You can view the available class mappings for the Service Graph Connector for Microsoft Defender for IoT (Azure) by navigating to **All** > **Service Graph for MSFT D4IoT (Azure)** > **Class Mappings**. In the class mappings table, you can view the following attributes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Class mapping attributes

Field	Description
Source Class	The device type from the source system (Azure).
Target CMDB class	The expected ServiceNow class for the CI.
OT Device type	The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example: An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is **server** and its device type is **HMI**. **Note:** In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select **No OT Function**. For OT devices where the device type is unknown, select **Unknown**.
Allow OS classification	When set to **True**, if an operating system is found on the CI, the target is switched away from the target CMDB class to a ServiceNow class that matches its OS.
Active	When checked, the class mapping is set to **Active**.

Computer [cmdb_ci_computer]

The following attributes in the Computer [cmdb_ci_computer] table are populated by collected data:

Computer [cmdb_ci_computer] attributes

Attribute label	Attribute name
Most recent discovery	last_discovered
Operating System	os
OS Address Width (bits)	os_address_width
OS Domain	os_domain
OS Version	os_version

External system metadata [cmdb_key_value_v2]

The following attributes in the External system metadata [cmdb_key_value_v2] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

External system metadata [cmdb_key_value_v2] attributes

Attribute label	Attribute name
Discovery source	discovery_source
Key	key
Source key	source_key
String value	string_value
URL value	url_value
Value type	value_type

Hardware [cmdb_ci_hardware]

The following attributes in the Hardware [cmdb_ci_hardware] table are populated by collected data:

Hardware [cmdb_ci_hardware] attributes

Attribute label	Attribute name
Class	sys_class_name
Model number	model_number
Most recent discovery	last_discovered
Location	location
Model ID	model_id
Manufacturer	manufacturer
First discovered	first_discovered
Owned by	owned_by
Approval group	change_control
Managed By Group	managed_by_group
Managed by	managed_by
Name	name
Company	company
Support group	support_group
Change Group	assignment_group
Assigned to	assigned_to
Supported by	supported_by

Relationships created for Hardware

Parent class	Relationship type	Child class
Hardware [cmdb_ci_hardware]	Owns::Owned by	IP Address [cmdb_ci_ip_address]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Relationships created for Hardware (continued)

Parent class	Relationship type	Child class
Hardware [cmdb_ci_hardware]	Owns::Owned by	Network Adapter [cmdb_ci_network_adapter]
Hardware [cmdb_ci_hardware]	Reference	External system metadata [cmdb_key_value_v2]
Hardware [cmdb_ci_hardware]	Reference	OT Device [cmdb_ot_entity]

IP Address [cmdb_ci_ip_address]

The following attributes in the IP Address [cmdb_ci_ip_address] table are populated by collected data:

IP Address [cmdb_ci_ip_address] attributes

Attribute label	Attribute name
IP Address	ip_address
IP version	ip_version
Owned By Configuration Item	owned_by_cmdb_ci

Relationships created for IP Address

Parent class	Relationship type	Child class
IP Address [cmdb_ci_ip_address]	Reference	Network Intrusion Detection System [cmdb_ci_nids]
IP Address [cmdb_ci_ip_address]	Reference	Hardware [cmdb_ci_hardware]

Network Adapter [cmdb_ci_network_adapter]

The following attributes in the Network Adapter [cmdb_ci_network_adapter] table are populated by collected data:

Network Adapter [cmdb_ci_network_adapter] attributes

Attribute label	Attribute name
MAC Address	mac_address
Name	name
Discovery source	discovery_source

Relationships created for Network Adapter

Parent class	Relationship type	Child class
Network Adapter [cmdb_ci_network_adapter]	Reference	Network Intrusion Detection System [cmdb_ci_nids]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Relationships created for Network Adapter (continued)

Parent class	Relationship type	Child class
Network Adapter [cmdb_ci_network_adapter]	Reference	Hardware [cmdb_ci_hardware]

Network Intrusion Detection System [cmdb_ci_nids]

The following attributes in the Network Intrusion Detection System [cmdb_ci_nids] table are populated by collected data:

Network Intrusion Detection System [cmdb_ci_nids] attributes

Attribute label	Attribute name
First discovered	first_discovered
NIDS source name	source_name
Life Cycle Stage	life_cycle_stage
Life Cycle Stage Status	life_cycle_stage_status
Name	name
Correlation ID	correlation_id
Firmware version	firmware_version
Fully qualified domain name	fqdn
NIDS assignment zone	zone
NIDS manager connection state	connection_state
Validated	validated
Manufacturer	manufacturer

Relationships created for NIDS

Parent class	Relationship type	Child class
Network Intrusion Detection System [cmdb_ci_nids]	Detects::Detected by	Hardware [cmdb_ci_hardware]
Network Intrusion Detection System [cmdb_ci_nids]	Owns::Owned by	IP Address [cmdb_ci_ip_address]
Network Intrusion Detection System [cmdb_ci_nids]	Owns::Owned by	Network Adapter [cmdb_ci_network_adapter]

Operational Technology (OT) [cmdb_ci_ot]

The following attributes in the Operational Technology (OT) [cmdb_ci_ot] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology (OT) [cmdb_ci_ot] attributes

Attribute label	Attribute name
Most recent discovery	last_discovered

OT Control Module [cmdb_ci_ot_control_module]

The following attributes in the OT Control Module [cmdb_ci_ot_control_module] table are populated by collected data:

OT Control Module [cmdb_ci_ot_control_module] attributes

Attribute label	Attribute name
Vendor	vendor
Support group	support_group
Serial number	serial_number
Class	sys_class_name
First discovered	first_discovered
Approval group	change_control
Managed by	managed_by
Managed By Group	managed_by_group
Change Group	assignment_group
Company	company
Rack number	rack_number
Slot number	slot_number
Location	location
Name	name
Firmware version	firmware_version
Most recent discovery	last_discovered
Assigned to	assigned_to
Owned by	owned_by
Supported by	supported_by
Model ID	model_id

Relationships created for OT Control Module

Parent class	Relationship type	Child class
OT Control Module [cmdb_ci_ot_control_module]	Reference	OT Device [cmdb_ot_entity]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Control System [cmdb_ci_ot_control]

The following attributes in the OT Control System [cmdb_ci_ot_control] table are populated by collected data:

OT Control System [cmdb_ci_ot_control] attributes

Attribute label	Attribute name
Has module	has_module
Most recent discovery	last_discovered

Relationships created for OT Control System

Parent class	Relationship type	Child class
OT Control System [cmdb_ci_ot_control]	Owns::Owned by	OT Control Module [cmdb_ci_ot_control_module]

OT Device [cmdb_ot_entity]

The following attributes in the OT Device [cmdb_ot_entity] table are populated by collected data:

OT Device [cmdb_ot_entity] attributes

Attribute label	Attribute name
ISA entity site	isa_entity_site
OT discovery source ID	ot_correlation_id
Device criticality	business_criticality
Purdue level	purdue_level
Zone	zone
OT device type	ot_asset_type
IRE criterion attribute	ire_criterion_attribute

PLC [cmdb_ci_ot_plc]

The following attributes in the PLC [cmdb_ci_ot_plc] table are populated by collected data:

PLC [cmdb_ci_ot_plc] attributes

Attribute label	Attribute name
Most recent discovery	last_discovered
Switch position	switch_position
Switch remote	switch_remote_mode

Serial Number [cmdb_serial_number]

The following attributes in the Serial Number [cmdb_serial_number] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Serial Number [cmdb_serial_number] attributes

Attribute label	Attribute name
Serial Number	serial_number
Serial Number Type	serial_number_type
Valid	valid

Relationships created for Serial Number

Parent class	Relationship type	Child class
Serial Number [cmdb_serial_number]	Reference	Hardware [cmdb_ci_hardware]
Network Adapter [cmdb_ci_network_adapter]	Reference	Hardware [cmdb_ci_hardware]

Attribute mapping and classification for Service Graph Connector for Microsoft Defender for IoT (Azure)

The following tables describe the attribute mapping and classification for sensors and devices.

Sensors attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	• sys_object_source • cmdb_ci_nids	• snk in sys_object_source • correlation_id	Unique ID for the sensor.
name	String	cmdb_ci_nids	name	Name of the sensor.
properties.hostname	String	cmdb_ci_nids	fqdn	Host name of the sensor.
properties.ip	String	cmdb_ci_ip_address	ip_address	IP address of the sensor.
properties.learningMode	Boolean	cmdb_ci_nids	False or unavailable: Life Cycle Stage (life_cycle_stage) : Operational Life Cycle Stage Status (life_cycle_stage_status): In Use	Learning mode status of the IoT sensor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sensors attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
			True: Life Cycle Stage (life_cycle_stage) : Operational Life Cycle Stage Status (life_cycle_stage_status): Learning	
properties.mac	String	cmdb_ci_network_adapter	mac_address	MAC address of the sensor.
properties.sensorStatus	String	cmdb_ci_nids	connection_state	Status of the IoT sensor.
properties.sensorVersion	String	cmdb_ci_nids	firmware_version	Version of the IoT sensor.
properties.upSince_date	Date and time as string	cmdb_ci_nids	first_discovered	Startup time.
properties.zone	String	cmdb_ci_nids	zone	Zone of the IoT sensor.

Devices attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/subscription-id>/providers/<providers-id>/location/<location>/deviceGroups/<device-Group>/devices/<name-field>	• sys_object_source • cmdb_ot_entity • cmdb_key_value_v2	• snk in sys_object_source • discovery_source_id in cmdb_ot_entity	Unique ID for the device.
resourceGroup	(Empty)	cmdb_key_value_v2	(Empty)	Resource group
tenantId	(Empty)	cmdb_key_value_v2	(Empty)	Tenant ID
properties.authorizedState	String	cmdb_key_value_v2	(Empty)	Authorized state of the device
properties.criticality	String	cmdb_ot_entity	business_criticality	Criticality of the device
properties.deviceName	String	cmdb_ci	name	Name of the device.
properties.deviceSubtypeDisplayName	String	cmdb_ci	sys_class_name	Device subtype display name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.firstSeen	Date and time as string	• cmdb_ci • cmdb_ci_ot_control_module (if control modules are present)	first_discovered	First time the device was seen.
properties.lastSeen	Date and time as string	• cmdb_ci • cmdb_ci_ot_control_module (if control modules are present)	most_recent_discovery	Last time the device was seen.
properties.purdueLevel	String	cmdb_ot_entity	purdue_level	Purdue level of the device.
properties.operatingSystem.distribution	String	cmdb_ci_computer	os	OS distribution
properties.operatingSystem.version	String	cmdb_ci_computer	os_version	OS version
properties.operatingSystem.platform	String	cmdb_ci_computer	os_domain	OS platform
properties.operatingSystem.architecture	String	cmdb_ci_computer	os_address_width	OS architecture
properties.additionalFields.plcKeyState	(Empty)	cmdb_ci_ot_plc	switch_position	PLC key state
properties.additionalFields.plcRunState	(Empty)	cmdb_ci_ot_plc	switch_remote_mode	PLC run state
properties.hardware	Object	(Empty)	(Empty)	Device hardware data
properties.hardware.model	String	cmdb_ci	(Empty)	Hardware model
properties.hardware.serialNumber	String	cmdb_serial_number	serial_number	Hardware serial number
properties.hardware.vendor	String	cmdb_ci	manufacturer	Hardware vendor
properties.nics	Array of Objects	(Empty)	(Empty)	List of the device network interface cards.
properties.nics[{}]	Object	(Empty)	(Empty)	Network interface card properties
properties.nics[{}].ipv4Address	String	cmdb_ci_ip_address	ip_address	IPv4 address
properties.nics[{}].macAddress	String	cmdb_ci_network_adapter	mac	MAC Address
properties.slots	Array of Objects	(Empty)	(Empty)	List of the device slot in the backplane.
properties.slots[{}]	Object	(Empty)	(Empty)	Slot data in PLC backplane.
properties.slots[{}].firmwareVersion	String	cmdb_ci_ot_control_module	firmware_version	Firmware version of the slot.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.slots[{}].model	String	cmdb_ci_ot_control_module	model_id	Model of the slot.
properties.slots[{}].rackNumber	Integer	cmdb_ci_ot_control_module	rack_number	Rack number in the backplane
properties.slots[{}].serialNumber	String	cmdb_ci_ot_control_module	serial_number	Serial number of the slot.
properties.slots[{}].slotNumber	Integer	cmdb_ci_ot_control_module	slot_number	Slot number inside the rack.
properties.slots[{}].hardwareVendor	String	cmdb_ci_ot_control_module	vendor	Hardware vendor of the slot.

Device type classification

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Alarm Siren	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Alarm System	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
ATM	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Backup Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Barcode Scanner	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DB Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
DCS Controller	Industrial	(Empty)	DCS	cmdb_ci_ot_dcs	NULL
Domain Controller	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Door Control Panel	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DVR	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Elevator	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Engineering Station	Industrial	(Empty)	EWS	cmdb_ci_ot_ews	EWS
Fire Alarm	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Fire Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Firewall	(Empty)	(Empty)	IP Firewall	cmdb_ci_ip_firewall	NULL
Game console	(Empty)	(Empty)	Game Console	cmdb_ci_game_console	NULL
Historian	(Empty)	(Empty)	Historian	cmdb_ci_ot_historian	Historian
HMI	Industrial	(Empty)	HMI	cmdb_ci_ot_hmi	HMI

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Humidity Sensor	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
HVAC	(Empty)	(Empty)	HVAC Equipment	cmdb_ci_hvac	NULL
I/O Adapter	(Empty)	(Empty)	Network Adapter	(Empty)	NA
IED	(Empty)	(Empty)	IED	cmdb_ci_ot_ied	ied
Industrial Packaging System	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Industrial Robot	(Empty)	(Empty)	Industrial Robot	cmdb_ci_ot_industrial_robot	Industrial Robot
Industrial Scale	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Intercom	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
IP Camera	(Empty)	(Empty)	IP Camera	cmdb_ci_ip_camera	NULL
IP Telephone	(Empty)	(Empty)	IP phone	cmdb_ci_ip_phone	NULL
Marquee	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Meter	(Empty)	(Empty)	Industrial Sensor	cmdb_ci_ot_industrial_sensor	Industrial Sensor
Motion Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Multicast/ Broadcast	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
NTP Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
People Counter System	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Physical Location	(Empty)	(Empty)	(Empty)	(Empty)	NULL
PLC	Industrial	(Empty)	PLC	cmdb_ci_ot_plc	PLC
Pneumatic Device	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Printer	(Empty)	(Empty)	Printer	cmdb_ci_printer	NULL
Protocol Converter	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Punch Clock	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Robot Controller	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
Router	(Empty)	(Empty)	IP Router	cmdb_ci_ip_router	NULL
RTU	(Empty)	(Empty)	RTU	cmdb_ci_ot_rtu	NULL
Server	Server	(Empty)	Server	cmdb_ci_server	NULL
Servo Drive	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Slot	(Empty)	(Empty)	OT Control Module	cmdb_ci_ot_control_module	OT Control Module
Smart Light	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart Phone	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Smart Switch	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart TV	(Empty)	(Empty)	Smart Television	cmdb_ci_stv	NULL
Storage	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Switch	Network Device	(Empty)	IP Switch	cmdb_ci_ip_switch	NULL
Tablet	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Terminal Station	(Empty)	(Empty)	Computer	cmdb_ci_computer	NULL
Thermostat	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Turnstile	(Empty)	(Empty)	IoT device	cmdb_ci_iot	
Uninterruptable Power Supply	(Empty)	(Empty)	UPS	cmdb_ci_ups	NULL
Variable Frequency Drive	(Empty)	(Empty)	Industrial Drive	cmdb_ci_ot_industrial_drive	Industrial Drive
VPN Gateway	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wifi Pineapple	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wireless Access Point	(Empty)	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL
WLAN access point	Network Device	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Workstation	Workstation	(Empty)	Computer	cmdb_ci_computer	NULL
Unknown	All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Unclassified	Unclassified or All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any other type	(Empty)	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any above type value except with designation Network and IoT	(Empty)	• windows server • windows server, version 2004[8] • windows server, version 1909[9] • windows server, version 1903[9] • windows server 2019 • windows server 2016 • windows server 2012 r2 • windows server 2012 • windows server 2008 r2 • windows server 2008 • windows server 2003 r2 • windows server 2003	Windows Server	cmdb_ci_linux_server	Same as when the operating system isn't present.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
		• windows 2000 server • windows nt 4.0 server • windows nt 3.51 server • windows nt 3.5 server • windows nt 3.1 server			
Any above type value except with designation Network and IoT	(Empty)	• linux • arch • centos • debian • fedora • suse • red hat • rhel • ubuntu • oracle	Linux Server	cmdb_ci_linux_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	aix	AIX Server	cmdb_ci_aix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	esx	ESX Server	cmdb_ci_esx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• hp/ux • hpux	HP-UX Server	cmdb_ci_hpux_server	Same as when the operating system isn't present.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Any above type value except with designation Network and IoT	(Empty)	• hyper-v • hyperv • hyper	HypverV Server	cmdb_ci_hyper_v_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• solaris • sunos • sun os	Solaris Server	cmdb_ci_solaris_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• macos x server • macos server • os x • osx	OSX Server	cmdb_ci_osx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• unix • gnu	Unix Server	cmdb_ci_unix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• win • windows • Microsoft • windows 1.0, 1.02, 1.03, 1.04, 2.03, 2.10, 2.11, 3.0, 3.1, 3.2, 7, 8, 8.1, 10, 98, 95 • windows 2000 • windows for workgroups 3.11 • windows me	Base Computer class	cmdb_ci_computer	Same as when the operating system isn't present.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
		• windows nt 3.1, 3.5, 3.51, 4.0 • windows vista • windows xp • windows xp professional x64 edition			
Any above type value except with designation Network and IoT	(Empty)	server	Base Server Class	cmdb_ci_server	Same as when the operating system isn't present.

Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

Integrate Microsoft Defender for IoT (On-premises Management Console) with the ServiceNow® Operational Technology Manager application to automate import of sensor appliances, OT devices, and network connections.

Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Supported versions

Microsoft Defender for IoT (On-premises Management Console) version: 10.5.2#br later

Use cases

You can use the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) with the ServiceNow® Operational Technology Manager application to import sensor appliances, OT devices, and network connections.

Guided setup

The guided setup for the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) provides an organized sequence of tasks to configure the integration on your instance. To access the guided setup, see Configure guided setup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

CMDB integrations dashboard

The Integration Commons for CMDB store app provides a dashboard with a central view of the status, processing results, and processing errors of all installed integrations. You can see metrics for all integration runs. You can filter the view to a specific CMDB integration, a specific time duration, or a specific integration run. For more details about monitoring integrations in the CMDB Integrations Dashboard, see Integration Commons for CMDB.

Data mapping

Data from the Microsoft Defender for IoT (On-premises Management Console) data sources is mapped and transformed into the ServiceNow CMDB Configuration Item (CI) class definitions using the Robust Transform Engine (RTE). Data is inserted into the ServiceNow CMDB using the Identification and Reconciliation Engine (IRE).

When you complete the setup, you can configure the integration to periodically pull data from the Microsoft Defender for IoT (On-premises Management Console) application.

The following table lists the data sources included for a Microsoft Defender for IoT (On-premises Management Console) project and the corresponding staging tables where the imported data is loaded.

Data sources and staging tables for Microsoft Defender for IoT (On-premises Management Console)

Data source	Staging table
SG-OT Microsoft D4IoT Connections Import	SG-OT Msft D4IoT Connections Import [sn_msftd4iotsgc_sg_ot_msft_d4iot_connections_import]
SG-OT Microsoft D4IoT Devices Import	SG-OT Msft D4IoT Devices Import [sn_msftd4iotsgc_sg_ot_msft_d4iot_devices_import]
SG-OT Microsoft D4IoT Sensors Import	SG-OT Msft D4IoT Sensors Import [sn_msftd4iotsgc_sg_ot_msft_d4iot_sensors_import]

The imported data from the staging tables is then inserted into the following target tables:

- AIX Server [cmdb_ci_aix_server]
- Computer [cmdb_ci_computer]
- Configuration Item [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX Server [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- External System Metadata [cmdb_key_value_v2]
- Game Console [cmdb_ci_game_console]
- Handheld Computing Device [cmdb_ci_handheld_computing]
- Historian [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX Server [cmdb_ci_hpux_server]
- HVAC Equipment [cmdb_ci_hvac]
- HyperV Server [cmdb_ci_hyper_v_server]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- IED [cmdb_ci_ot_ied]
- Industrial Actuator [cmdb_ci_ot_industrial_actuator]
- Industrial Drive [cmdb_ci_ot_industrial_drive]
- Industrial Robot [cmdb_ci_ot_industrial_robot]
- Industrial Sensor [cmdb_ci_ot_industrial_sensor]
- IoT Device [cmdb_ci_iot]
- IP Address [cmdb_ci_ip_address]
- IP Camera [cmdb_ci_ip_camera]
- IP Firewall [cmdb_ci_ip_firewall]
- IP Phone [cmdb_ci_ip_phone]
- Linux Server [cmdb_ci_linux_server]
- Netgear [cmdb_ci_netgear]
- Network Adapter [cmdb_ci_network_adapter]
- Network Intrusion Detection System [cmdb_ci_nids]
- Operational Technology (OT) [cmdb_ci_ot]
- OSX Server [cmdb_ci_osx_server]
- OT Control Module [cmdb_ci_ot_control_module]
- OT Control System [cmdb_ci_ot_control]
- OT Device Details [cmdb_ot_entity]
- OT Field Device [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- Printer [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- Serial Number [cmdb_serial_number]
- Server [cmdb_ci_server]
- Server [cmdb_ci_server]
- Solaris Server [cmdb_ci_solaris_server]
- Source [sys_object_source]
- Unix Servercmdb_ci_unix_server]
- Uninterruptible Power Supply (UPS) [cmdb_ci_ups]
- Wireless Access Point [cmdb_ci_wap_network]

For more information on where data is saved when pulling data from a Microsoft Defender for IoT (On-premises Management Console) project, see CMDB classes targeted.

Configure the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

Use the Guided Setup for the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) to lead you through the integration steps.

Before you begin

Dependencies and requirements:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Integration Commons for CMDB store app, which is automatically installed.
- The CMDB CI Class Models app, which is automatically installed.
- The ITOM Discovery License plugin (com.snc.itom.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.itom.license). For more information, see Request Discovery.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.

Role required: admin

Note: If you have an earlier version of the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console), then don't migrate data from the old connector. You must uninstall the previous version and run the new integration.

Procedure

1. Ensure that the application scope is set to the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console) application by using the application picker.
   For more information, see Application picker.
2. Navigate to **All** > **Service Graph Connector Microsoft D4IoT** > **Guided Setup**.
3. On the Getting started page, select **Get Started**.
4. To configure a MID Server, complete the following:
   a. In the Setup Connections and Credentials section, select the Configure MID server task.
   b. Select **Mark as complete** once you complete the MID Server configuration linked in the description.
5. To update the Connection and Credentials Alias record, complete the following:
   a. In the Setup Connections and Credentials section, select the Connections and Credentials task.
   b. Select **Configure**.
   c. Open the default record **Microsoft D4IoT Base API**.
   d. From the Connections related list, select **New** to create a new HTTP(s) Connection record.
   e. In the **Connection URL** field, enter the name for the URL of your Microsoft Defender for IoT Central Manager.
   For example, `https://192.168.1.100`.
   f. **Optional:** If you are using a MID Server, select all of the following:
      - **Use MID Server** box
      - **MID Server** from the Advanced MID Server Configuration related list
      - **MID Selection** from the list
   g. In the **Credential** field, select the search icon to open the Credentials records list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

h. Select **New** to create a new record.

i. Select the **API Key Credentials** type.

j. In the **API Key** field, enter a name and the API Key provided by your Microsoft Defender for IoT management console.

k. Select **Submit** to create the credential record.
To create an API Key in the Microsoft Defender for IoT management console, refer to Microsoft product documentation: https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis.

l. On the Connection form, select **Submit** to finish creating the Connection record.

6. To test the connection, complete the following:

a. In the Setup Connections and Credentials section, select the Test/Validate Connection task.

b. Select the **Test Connection** UI action from the related links section on the data source record for sensors.
After completing the connection test, view the results. You must perform the suggested troubleshooting steps until the test result returns **Success**.

c. Check that the connection manager has a valid certificate.

A valid certificate must be installed for a production environment. For a non-production or proof of concept (POC) instance, you can configure the system properties to enable the integration to work when the connection manager doesn't have a valid certificate. The following table lists the system properties that you can configure for a non-production environment.

System properties for a non-production environment

Property	Value
com.glide.communications.httpclient.verify_hostname	Set to **false**.
com.glide.communications.httpclient.verify_revoked_certificate	Set to **false**. If you need to add this system property, see Add a system property.
com.glide.communications.trustmanager_trustall	Set to **true**.

d. Check the MID security policy.
In the intranet record, verify that the columns in the following table show the specified values.

Intranet record values

Column	Value
Certificate chain check	**false**
Hostname check	**false**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Value
Revocation check	**false**

For more information, see MID Server certificate check policies.

The connection shows that it is set correctly when the progress window shows the Completion code **Success**, and the number of records processed shows as the same number of sensors in the connection manager.

7. To configure the system properties, complete the following:

   a. In the Configure System Properties section, select **Configure**.

   b. Configure the following system properties.

Property	Description
sn_msftd4iotsgc.resourcepath.sensor	Set the sensors resource path. ▪ The sensors resource path is provided by default for the V3 API version. ▪ If you want to use a different API version, you can override the path.
sn_msftd4iotsgc.resourcepath.device	▪ The devices resource path is provided by default for the V3 API version. ▪ If you want to use a different API version, you can override the path.
sn_msftd4iotsgc.resourcepath.connection	▪ The connections resource path is provided by default for the V3 API version. ▪ If you want to use a different API version, you can override the path.
sn_msftd4iotsgc.pagesize.device	Enter the number of records to display per page for each Devices and Connections API. Default value: 50 records per page
sn_msftd4iotsgc.pagesize.connection	▪ If you want to use a different Connection Alias than the Microsoft D4IoT Base API configured while setting up the connections and credentials records, you can enter the sys_id of your custom Connection Alias record in this property field. ▪ The default value of this property is empty. If this property field is left blank, the Microsoft D4IoT Base API Connection Alias is used by default.
sn_msftd4iotsgc.get_all_devices	Select whether to fetch all records for devices, or only new records since the start time of the last successful import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Property	Description
	Note: When you import devices for the first time, all records are imported regardless of the setting for this property.
sn_msftd4iotsgc.get_all_connections	Select whether to fetch all records for connections, or only new records since the start time of the last successful import in the CMDB. **Note:** When you import connections for the first time, all records are imported regardless of the setting for this property.
sn_msftd4iotsgc.ot.vr.integration.id	If you are using the Operational Technology Vulnerability Response application with the Service Graph for Microsoft Defender for IoT integration, provide the sys ID of the OT VR import record. **Note:** If the Operational Technology Vulnerability Response plugin is installed and this property field is left blank, the **Microsoft D4IoT Devices CVE Integration (Delta Import)** executes if Active is set to **true** on the record.

c. Select **Save**.

8. To import sensors, complete the following:
   a. In the Configure Sensors (NIDS) section, select the Import Sensors task.
   b. Select **Configure**.
   c. Select **Active** to activate the Scheduled Data Import job.
9. To configure the NIDS, complete the following:
   a. In the Configure Sensors (NIDS) section, select the Import Sensors task.
   b. Select **Mark as complete** once you complete the NIDS configuration linked in the description.
10. To configure import schedules, complete the following:
    a. In the Configure Import Schedules section, select **Configure**.
    b. Select **SG-OT Microsoft D4IoT Sensors Scheduled Import** to review or change the sensors import schedule as needed.
       - By default, the sensors import schedule is configured to run daily at midnight.
       - Import sensors before importing devices or connections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Select **Active** to activate the sensors import schedule.

d. Select **SG-OT Microsoft D4IoT Devices Scheduled Import** to review or change the devices import schedule as needed.
   - By default, the devices import schedule is configured to run daily at midnight.
   - Devices are queried by sensor. The Service Graph Connector queries for devices detected by validated sensors. For information about configuring Network Intrusion Detection System (NIDS) appliances, see Validate the NIDS.

e. Select **Active** to activate the devices import schedule.

f. Select **SG-OT Microsoft D4IoT Connections Scheduled Import** to review or change the connections import schedule as needed.
   - By default, the connections import schedule is configured to run after the devices import runs (**After Parent Runs**).
   - Connections are only imported if both devices (Source & Destination in Microsoft API, or Parent & Child in the CMDB) are already in the CMDB.
   - Import devices before importing connections.

CMDB classes targeted in the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

When you complete the guided setup, you can configure the integration to periodically pull data from a Microsoft Defender for IoT (On-premises Management Console) project. The data is saved in tables that extend from the Configuration item [cmdb_ci] table.

Computer [cmdb_ci_computer]

The following attributes in the Computer [cmdb_ci_computer] table are populated by collected data:

Computer [cmdb_ci_computer] attributes

Attribute label	Attribute name
Most recent discovery	last_discovered
Operating System	os
OS Address Width (bits)	os_address_width
OS Domain	os_domain
OS Version	os_version

External system metadata [cmdb_key_value_v2]

The following attributes in the External system metadata [cmdb_key_value_v2] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

External system metadata [cmdb_key_value_v2] attributes

Attribute label	Attribute name
Discovery source	discovery_source
Key	key
Source key	source_key
String value	string_value
URL value	url_value
Value type	value_type

Hardware [cmdb_ci_hardware]

The following attributes in the Hardware [cmdb_ci_hardware] table are populated by collected data:

Hardware [cmdb_ci_hardware] attributes

Attribute label	Attribute name
Class	sys_class_name
Model number	model_number
Most recent discovery	last_discovered
Location	location
Model ID	model_id
Manufacturer	manufacturer
First discovered	first_discovered
Owned by	owned_by
Approval group	change_control
Managed By Group	managed_by_group
Managed by	managed_by
Name	name
Company	company
Support group	support_group
Change Group	assignment_group
Assigned to	assigned_to
Supported by	supported_by

Relationships created for Hardware

Parent class	Relationship type	Child class
Hardware [cmdb_ci_hardware]	Owns::Owned by	IP Address [cmdb_ci_ip_address]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Relationships created for Hardware (continued)

Parent class	Relationship type	Child class
Hardware [cmdb_ci_hardware]	Owns::Owned by	Network Adapter [cmdb_ci_network_adapter]
Hardware [cmdb_ci_hardware]	Reference	External system metadata [cmdb_key_value_v2]
Hardware [cmdb_ci_hardware]	Reference	OT Device [cmdb_ot_entity]

IP Address [cmdb_ci_ip_address]

The following attributes in the IP Address [cmdb_ci_ip_address] table are populated by collected data:

IP Address [cmdb_ci_ip_address] attributes

Attribute label	Attribute name
IP Address	ip_address
IP version	ip_version
Owned By Configuration Item	owned_by_cmdb_ci

Relationships created for IP Address

Parent class	Relationship type	Child class
IP Address [cmdb_ci_ip_address]	Reference	Network Intrusion Detection System [cmdb_ci_nids]
IP Address [cmdb_ci_ip_address]	Reference	Hardware [cmdb_ci_hardware]

Network Adapter [cmdb_ci_network_adapter]

The following attributes in the Network Adapter [cmdb_ci_network_adapter] table are populated by collected data:

Network Adapter [cmdb_ci_network_adapter] attributes

Attribute label	Attribute name
MAC Address	mac_address
Name	name
Discovery source	discovery_source

Relationships created for Network Adapter

Parent class	Relationship type	Child class
Network Adapter [cmdb_ci_network_adapter]	Reference	Network Intrusion Detection System [cmdb_ci_nids]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Relationships created for Network Adapter (continued)

Parent class	Relationship type	Child class
Network Adapter [cmdb_ci_network_adapter]	Reference	Hardware [cmdb_ci_hardware]

Network Intrusion Detection System [cmdb_ci_nids]

The following attributes in the Network Intrusion Detection System [cmdb_ci_nids] table are populated by collected data:

Network Intrusion Detection System [cmdb_ci_nids] attributes

Attribute label	Attribute name
First discovered	first_discovered
NIDS source name	source_name
Life Cycle Stage	life_cycle_stage
Life Cycle Stage Status	life_cycle_stage_status
Name	name
Correlation ID	correlation_id
Firmware version	firmware_version
Fully qualified domain name	fqdn
NIDS assignment zone	zone
NIDS manager connection state	connection_state
Validated	validated
Manufacturer	manufacturer

Relationships created for NIDS

Parent class	Relationship type	Child class
Network Intrusion Detection System [cmdb_ci_nids]	Detects::Detected by	Hardware [cmdb_ci_hardware]
Network Intrusion Detection System [cmdb_ci_nids]	Owns::Owned by	IP Address [cmdb_ci_ip_address]
Network Intrusion Detection System [cmdb_ci_nids]	Owns::Owned by	Network Adapter [cmdb_ci_network_adapter]

Operational Technology (OT) [cmdb_ci_ot]

The following attributes in the Operational Technology (OT) [cmdb_ci_ot] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology (OT) [cmdb_ci_ot] attributes

Attribute label	Attribute name
Most recent discovery	last_discovered

OT Control Module [cmdb_ci_ot_control_module]

The following attributes in the OT Control Module [cmdb_ci_ot_control_module] table are populated by collected data:

OT Control Module [cmdb_ci_ot_control_module] attributes

Attribute label	Attribute name
Vendor	vendor
Support group	support_group
Serial number	serial_number
Class	sys_class_name
First discovered	first_discovered
Approval group	change_control
Managed by	managed_by
Managed By Group	managed_by_group
Change Group	assignment_group
Company	company
Rack number	rack_number
Slot number	slot_number
Location	location
Name	name
Firmware version	firmware_version
Most recent discovery	last_discovered
Assigned to	assigned_to
Owned by	owned_by
Supported by	supported_by
Model ID	model_id

Relationships created for OT Control Module

Parent class	Relationship type	Child class
OT Control Module [cmdb_ci_ot_control_module]	Reference	OT Device [cmdb_ot_entity]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Control System [cmdb_ci_ot_control]

The following attributes in the OT Control System [cmdb_ci_ot_control] table are populated by collected data:

OT Control System [cmdb_ci_ot_control] attributes

Attribute label	Attribute name
Has module	has_module
Most recent discovery	last_discovered

Relationships created for OT Control System

Parent class	Relationship type	Child class
OT Control System [cmdb_ci_ot_control]	Owns::Owned by	OT Control Module [cmdb_ci_ot_control_module]

OT Device [cmdb_ot_entity]

The following attributes in the OT Device [cmdb_ot_entity] table are populated by collected data:

OT Device [cmdb_ot_entity] attributes

Attribute label	Attribute name
ISA entity site	isa_entity_site
OT discovery source ID	ot_correlation_id
Device criticality	business_criticality
Purdue level	purdue_level
Zone	zone
OT device type	ot_asset_type

PLC [cmdb_ci_ot_plc]

The following attributes in the PLC [cmdb_ci_ot_plc] table are populated by collected data:

PLC [cmdb_ci_ot_plc] attributes

Attribute label	Attribute name
Most recent discovery	last_discovered
Switch position	switch_position
Switch remote	switch_remote_mode

Serial Number [cmdb_serial_number]

The following attributes in the Serial Number [cmdb_serial_number] table are populated by collected data:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Serial Number [cmdb_serial_number] attributes

Attribute label	Attribute name
Serial Number	serial_number
Serial Number Type	serial_number_type
Valid	valid

Relationships created for Serial Number

Parent class	Relationship type	Child class
Serial Number [cmdb_serial_number]	Reference	Hardware [cmdb_ci_hardware]
Network Adapter [cmdb_ci_network_adapter]	Reference	Hardware [cmdb_ci_hardware]

Attribute mapping and classification for the Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console)

The following tables describe the attribute mapping and classification for sensors and devices.

Sensors attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	• sys_object_source • cmdb_ci_nids	• snk in sys_object_source • correlation_id	Unique ID for the sensor.
name	String	cmdb_ci_nids	name	Name of the sensor.
properties.hostname	String	cmdb_ci_nids	fqdn	Host name of the sensor.
properties.ip	String	cmdb_ci_ip_address	ip_address	IP address of the sensor.
properties.learningMode	Boolean	cmdb_ci_nids	False or unavailable: Life Cycle Stage (life_cycle_stage) : Operational Life Cycle Stage Status (life_cycle_stage_status): In Use	Learning mode status of the IoT sensor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sensors attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
			True: Life Cycle Stage (life_cycle_stage) : Operational Life Cycle Stage Status (life_cycle_stage_status): Learning	
properties.mac	String	cmdb_ci_network_adapter	mac_address	MAC address of the sensor.
properties.sensorStatus	String	cmdb_ci_nids	connection_state	Status of the IoT sensor.
properties.sensorVersion	String	cmdb_ci_nids	firmware_version	Version of the IoT sensor.
properties.upSince_date	Date and time as string	cmdb_ci_nids	first_discovered	Startup time.
properties.zone	String	cmdb_ci_nids	zone	Zone of the IoT sensor.

Devices attribute mapping

Payload field name	Data type	Mapped to table	Mapped to field	Description
id	String format: /subscriptions/subscription-id>/providers/<providers-id>/location/<location>/deviceGroups/<device-Group>/devices/<name-field>	• sys_object_source • cmdb_ot_entity • cmdb_key_value_v2	• snk in sys_object_source • discovery_source_id in cmdb_ot_entity	Unique ID for the device.
resourceGroup	(Empty)	cmdb_key_value_v2	(Empty)	Resource group
tenantId	(Empty)	cmdb_key_value_v2	(Empty)	Tenant ID
properties.authorizedState	String	cmdb_key_value_v2	(Empty)	Authorized state of the device
properties.criticality	String	cmdb_ot_entity	business_criticality	Criticality of the device
properties.deviceName	String	cmdb_ci	name	Name of the device.
properties.deviceSubtypeDisplayName	String	cmdb_ci	sys_class_name	Device subtype display name.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.firstSeen	Date and time as string	• cmdb_ci • cmdb_ci_ot_control_module (if control modules are present)	first_discovered	First time the device was seen.
properties.lastSeen	Date and time as string	• cmdb_ci • cmdb_ci_ot_control_module (if control modules are present)	most_recent_discovery	Last time the device was seen.
properties.purdueLevel	String	cmdb_ot_entity	purdue_level	Purdue level of the device.
properties.operatingSystem.distribution	String	cmdb_ci_computer	os	OS distribution
properties.operatingSystem.version	String	cmdb_ci_computer	os_version	OS version
properties.operatingSystem.platform	String	cmdb_ci_computer	os_domain	OS platform
properties.operatingSystem.architecture	String	cmdb_ci_computer	os_address_width	OS architecture
properties.additionalFields.plcKeyState	(Empty)	cmdb_ci_ot_plc	switch_position	PLC key state
properties.additionalFields.plcRunState	(Empty)	cmdb_ci_ot_plc	switch_remote_mode	PLC run state
properties.hardware	Object	(Empty)	(Empty)	Device hardware data
properties.hardware.model	String	cmdb_ci	(Empty)	Hardware model
properties.hardware.serialNumber	String	cmdb_serial_number	serial_number	Hardware serial number
properties.hardware.vendor	String	cmdb_ci	manufacturer	Hardware vendor
properties.nics	Array of Objects	(Empty)	(Empty)	List of the device network interface cards.
properties.nics[{}]	Object	(Empty)	(Empty)	Network interface card properties
properties.nics[{}].ipv4Address	String	cmdb_ci_ip_address	ip_address	IPv4 address
properties.nics[{}].macAddress	String	cmdb_ci_network_adapter	mac	MAC Address
properties.slots	Array of Objects	(Empty)	(Empty)	List of the device slot in the backplane.
properties.slots[{}]	Object	(Empty)	(Empty)	Slot data in PLC backplane.
properties.slots[{}].firmwareVersion	String	cmdb_ci_ot_control_module	firmware_version	Firmware version of the slot.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Devices attribute mapping (continued)

Payload field name	Data type	Mapped to table	Mapped to field	Description
properties.slots[{}].model	String	cmdb_ci_ot_control_module	model_id	Model of the slot.
properties.slots[{}].rackNumber	Integer	cmdb_ci_ot_control_module	rack_number	Rack number in the backplane
properties.slots[{}].serialNumber	String	cmdb_ci_ot_control_module	serial_number	Serial number of the slot.
properties.slots[{}].slotNumber	Integer	cmdb_ci_ot_control_module	slot_number	Slot number inside the rack.
properties.slots[{}].hardwareVendor	String	cmdb_ci_ot_control_module	vendor	Hardware vendor of the slot.

Device type classification

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Alarm Siren	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Alarm System	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
ATM	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Backup Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Barcode Scanner	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DB Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
DCS Controller	Industrial	(Empty)	DCS	cmdb_ci_ot_dcs	NULL
Domain Controller	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Door Control Panel	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
DVR	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Elevator	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Engineering Station	Industrial	(Empty)	EWS	cmdb_ci_ot_ews	EWS
Fire Alarm	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Fire Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Firewall	(Empty)	(Empty)	IP Firewall	cmdb_ci_ip_firewall	NULL
Game console	(Empty)	(Empty)	Game Console	cmdb_ci_game_console	NULL
Historian	(Empty)	(Empty)	Historian	cmdb_ci_ot_historian	Historian
HMI	Industrial	(Empty)	HMI	cmdb_ci_ot_hmi	HMI

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Humidity Sensor	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
HVAC	(Empty)	(Empty)	HVAC Equipment	cmdb_ci_hvac	NULL
I/O Adapter	(Empty)	(Empty)	Network Adapter	(Empty)	NA
IED	(Empty)	(Empty)	IED	cmdb_ci_ot_ied	ied
Industrial Packaging System	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Industrial Robot	(Empty)	(Empty)	Industrial Robot	cmdb_ci_ot_industrial_robot	Industrial Robot
Industrial Scale	(Empty)	(Empty)	OT Field Device	cmdb_ci_ot_field_device	OT Field Device
Intercom	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
IP Camera	(Empty)	(Empty)	IP Camera	cmdb_ci_ip_camera	NULL
IP Telephone	(Empty)	(Empty)	IP phone	cmdb_ci_ip_phone	NULL
Marquee	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Meter	(Empty)	(Empty)	Industrial Sensor	cmdb_ci_ot_industrial_sensor	Industrial Sensor
Motion Detector	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Multicast/ Broadcast	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
NTP Server	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
People Counter System	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Physical Location	(Empty)	(Empty)	(Empty)	(Empty)	NULL
PLC	Industrial	(Empty)	PLC	cmdb_ci_ot_plc	PLC
Pneumatic Device	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Printer	(Empty)	(Empty)	Printer	cmdb_ci_printer	NULL
Protocol Converter	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Punch Clock	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Robot Controller	(Empty)	(Empty)	OT Control System	cmdb_ci_ot_control	OT Control System
Router	(Empty)	(Empty)	IP Router	cmdb_ci_ip_router	NULL
RTU	(Empty)	(Empty)	RTU	cmdb_ci_ot_rtu	NULL
Server	Server	(Empty)	Server	cmdb_ci_server	NULL
Servo Drive	(Empty)	(Empty)	Industrial Actuator	cmdb_ci_ot_industrial_actuator	Industrial Actuator
Slot	(Empty)	(Empty)	OT Control Module	cmdb_ci_ot_control_module	OT Control Module
Smart Light	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart Phone	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Smart Switch	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Smart TV	(Empty)	(Empty)	Smart Television	cmdb_ci_stv	NULL
Storage	(Empty)	(Empty)	Server	cmdb_ci_server	NULL
Switch	Network Device	(Empty)	IP Switch	cmdb_ci_ip_switch	NULL
Tablet	(Empty)	(Empty)	Handheld Computing Device	cmdb_ci_handheld_computing	NULL
Terminal Station	(Empty)	(Empty)	Computer	cmdb_ci_computer	NULL
Thermostat	(Empty)	(Empty)	IoT device	cmdb_ci_iot	NULL
Turnstile	(Empty)	(Empty)	IoT device	cmdb_ci_iot	
Uninterruptable Power Supply	(Empty)	(Empty)	UPS	cmdb_ci_ups	NULL
Variable Frequency Drive	(Empty)	(Empty)	Industrial Drive	cmdb_ci_ot_industrial_drive	Industrial Drive
VPN Gateway	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wifi Pineapple	(Empty)	(Empty)	Netgear	cmdb_ci_netgear	NULL
Wireless Access Point	(Empty)	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL
WLAN access point	Network Device	(Empty)	Wireless Access Point	cmdb_ci_wap_network	NULL

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Workstation	Workstation	(Empty)	Computer	cmdb_ci_computer	NULL
Unknown	All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Unclassified	Unclassified or All	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any other type	(Empty)	(Empty)	Operational Technology (OT)	cmdb_ci_ot	Operational Technology (OT)
Any above type value except with designation Network and IoT	(Empty)	• windows server • windows server, version 2004[8] • windows server, version 1909[9] • windows server, version 1903[9] • windows server 2019 • windows server 2016 • windows server 2012 r2 • windows server 2012 • windows server 2008 r2 • windows server 2008 • windows server 2003 r2 • windows server 2003	Windows Server	cmdb_ci_linux_server	Same as when the operating system isn't present.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
		• windows 2000 server • windows nt 4.0 server • windows nt 3.51 server • windows nt 3.5 server • windows nt 3.1 server			
Any above type value except with designation Network and IoT	(Empty)	• linux • arch • centos • debian • fedora • suse • red hat • rhel • ubuntu • oracle	Linux Server	cmdb_ci_linux_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	aix	AIX Server	cmdb_ci_aix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	esx	ESX Server	cmdb_ci_esx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• hp/ux • hpux	HP-UX Server	cmdb_ci_hpux_server	Same as when the operating system isn't present.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
Any above type value except with designation Network and IoT	(Empty)	• hyper-v • hyperv • hyper	HypverV Server	cmdb_ci_hyper_v_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• solaris • sunos • sun os	Solaris Server	cmdb_ci_solaris_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• macos x server • macos server • os x • osx	OSX Server	cmdb_ci_osx_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• unix • gnu	Unix Server	cmdb_ci_unix_server	Same as when the operating system isn't present.
Any above type value except with designation Network and IoT	(Empty)	• win • windows • Microsoft • windows 1.0, 1.02, 1.03, 1.04, 2.03, 2.10, 2.11, 3.0, 3.1, 3.2, 7, 8, 8.1, 10, 98, 95 • windows 2000 • windows for workgroups 3.11 • windows me	Base Computer class	cmdb_ci_computer	Same as when the operating system isn't present.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Device type classification (continued)

Microsoft Azure device sub type name	Microsoft Azure device type name	Operating system/ firmware	NOW class	NOW table	NOW OT type
		• windows nt 3.1, 3.5, 3.51, 4.0 • windows vista • windows xp • windows xp professional x64 edition			
Any above type value except with designation Network and IoT	(Empty)	server	Base Server Class	cmdb_ci_server	Same as when the operating system isn't present.

Using the Operational Technology Manager

After completing setup tasks, perform the following tasks to create foundational data and relationships for the ServiceNow® Operational Technology solution.

Task	Purpose
1. Populate a Microsoft Excel spreadsheet with your existing Operational Technology data.	Positions your existing data in the correct columns on a Microsoft Excel spreadsheet to ensure the success of your data upload.
2. Import your Excel spreadsheet.	Uploads your existing Operational Technology data to the Configuration Management Database (CMDB).
3. Run the Discovery for Operational Technology function.	Discovers Operational Technology (OT) devices in designated Purdue levels in your Industrial Control System (ICS) networks
4. Use the selections on the Operational Technology (OT) menu.	Enables editing or viewing detailed information for the OT devices in your enterprise.

Use the OT Manager Foundation

You can search for Operational Technology (OT) configuration items (CIs) and OT device information using the Operational Technology (OT) Manager Foundation.

Search for related records in an OT CMDB table

Search for Operational Technology (OT) configuration items (CIs) and OT device information available in an OT CMDB table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- The ServiceNow Otto panel must be activated. For more information, see Activate the panel standard chat.
- You must be assigned the now_assist_panel_user role to have access to the ServiceNow Otto panel.
- You must be assigned appropriate roles to search the relevant OT CMDB tables, such as cmdb_ot_viewer or cmdb_ot_isa_viewer.

Role required: now_assist_panel_user and cmdb_ot_viewer

About this task

The OT CMDB search feature uses the following:

- ServiceNow Otto for CMDB's Search CMDB agentic workflow

> **Important:** This agentic workflow is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

- ServiceNow AI Platform's Analytics Query Generator skill

> **Important:** This generative AI skill is turned on by default. The skill will be automatically available to appropriate role users for the application. For more information, see AI agents, skills, and agentic workflows on by default.

Procedure

1. Select the **ServiceNow Otto** icon.
   The ServiceNowOtto panel is displayed.
2. Enter a prompt such as `Search CMDB` or `CMDB Search` to search for OT CMDB tables.
   The command initiates a search of the CMDB tables.
3. Search for an OT device.
   To optimize search results, include OT-specific trigger words or device types in your query, such as `OT`, `Operational Technology`, PLC, or `HMI`. Using relevant OT trigger words helps the CMDB search agentic workflow identify the OT context and display results in the Industrial Workspace.

   For example, you can search for OT device information using prompts such as:

   - `Search for OT PLCs`
   - `Search for OT network gear with Purdue Level 3`
   - `Search for critical OT control systems`

Result

If fewer than five device records appear in the search results, the panel displays the devices. You can enter the OT device name for more information. The agent then gives you the option to view the device in either a form view or a unified map.

When more than five OT device records appear in the search results based on your search criteria, you can select the link in the panel to view them.

Agentic AI for the Operational Technology Manager

The Operational Technology (OT) Manager Foundation AI agent operates within agentic workflows to complete tasks autonomously.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Available agentic workflows for OTM AI agent collection

Agentic workflow name	Description	Available AI agents
Import OT device spreadsheet into OT CMDB	With the Import OT device spreadsheet into OT CMDB agentic workflow, you can do the following: • Import the device inventory spreadsheet and map data to the OT staging table • Validate OT staging table records, remediate invalid records, and import all validated records into the Configuration Management Database (CMDB)	OT Excel import task AI agent

Important: Some generative AI skills, AI agents, and agentic workflows are turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

Supported Large Language Models

Note:

You can use Now LLM Service, Azure OpenAI, Google Gemini or Anthropic Claude on AWS as the AI model provider for all generative AI skills and AI agents. Use the Configuration Controls in AI Control Tower to define which options are available, then set the skill-level preferences in the AI Admin Hub console. For more information, see Large language models on the ServiceNow AI Platform.

Security implementation considerations

Enable security implementation to execute AI agents and agentic workflows through Access Control Lists (ACLs) and user identities. For more information, see Implement access control in AI agents.

Considerations for running the autonomous AI agents

Important: By default, all agent workflow and AI agent records are read-only.

To run the AI agents autonomously, you must first duplicate the agentic workflow, and then proceed with the following steps:

- Activate the agentic workflow.
- Activate all agents within the agentic workflow.
- Activate the trigger to invoke the agentic workflow automatically. The triggers for each agentic workflow must be unique. If you prefer to invoke it manually, activating the trigger isn't necessary.

Standalone AI agents

There might be AI agents installed on your instance that are not used in agentic workflows. To learn how to see all agents that are available to you, see Find AI agents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role masking

Agentic workflows and their AI agents use role masking to determine which users can access them. Ones installed with your applications have specific roles that come included with the application. If you select *`Users with specific roles`* for user access, you must configure the security controls to include these roles. For the instructions to change the security controls, see Define security controls for an agentic workflow.

Import the OT device spreadsheet into OT CMDB agentic workflow

The Import OT device spreadsheet into OT CMDB agentic workflow automates the upload, validation, and import of OT device data into the OT CMDB.

Import OT device spreadsheet into OT CMDB overview

Using the Import OT device spreadsheet into OT CMDB agentic workflow, you can import the OT device inventory spreadsheet and map the spreadsheet data to the OT staging table. After importing and creating an OT staging table record, you can validate the staging record, remediate invalid records, and import all the validated records into the OT CMDB. For more information about how to use this agentic workflow, see Upload, validate, and import the OT device inventory spreadsheet.

Important: This agentic workflow is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

To modify the Import OT device spreadsheet into OT CMDB agentic workflow, duplicate it, and adjust the settings according to your requirements.

Important: When you modify an agentic workflow, AI agent, or a tool, update all instructions accordingly.

Import OT device spreadsheet into OT CMDB agentic workflow

The workflow helps you complete the following process:

1. Import the OT device inventory spreadsheet with an OT Excel SGC Import Task record.
2. Map the spreadsheet data to the SG OT Excel Stagings table.
3. Validate the OT staging table records.
4. Remediate invalid records if needed.
5. Import all validated records into the OT CMDB.

To access the agentic workflow:

1. Navigate to **All** > **AI Agent Studio** > **Agentic Solutions**.
2. Under the **Agentic workflows** tab, select the **Import OT device spreadsheet into OT CMDB** agentic workflow.

AI agents used in the Import OT device spreadsheet into OT CMDB agentic workflow

The Import OT device spreadsheet into OT CMDB agentic workflow uses the OT Excel import task AI agent. After you upload the device inventory spreadsheet, the agent processes the spreadsheet, creates an OT Excel SGC Import Task record, and maps the data to the SG OT Excel Stagings table. The agent then runs validations on the staging records, creates a remediation task for all invalid records, and imports the valid records into the OT CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: This AI agent is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

Upload, validate, and import the OT device inventory spreadsheet

Chat with an AI agent in the ServiceNowOtto panel to begin the process for uploading, validating, and importing your Operational Technology (OT) device data into the OT CMDB.

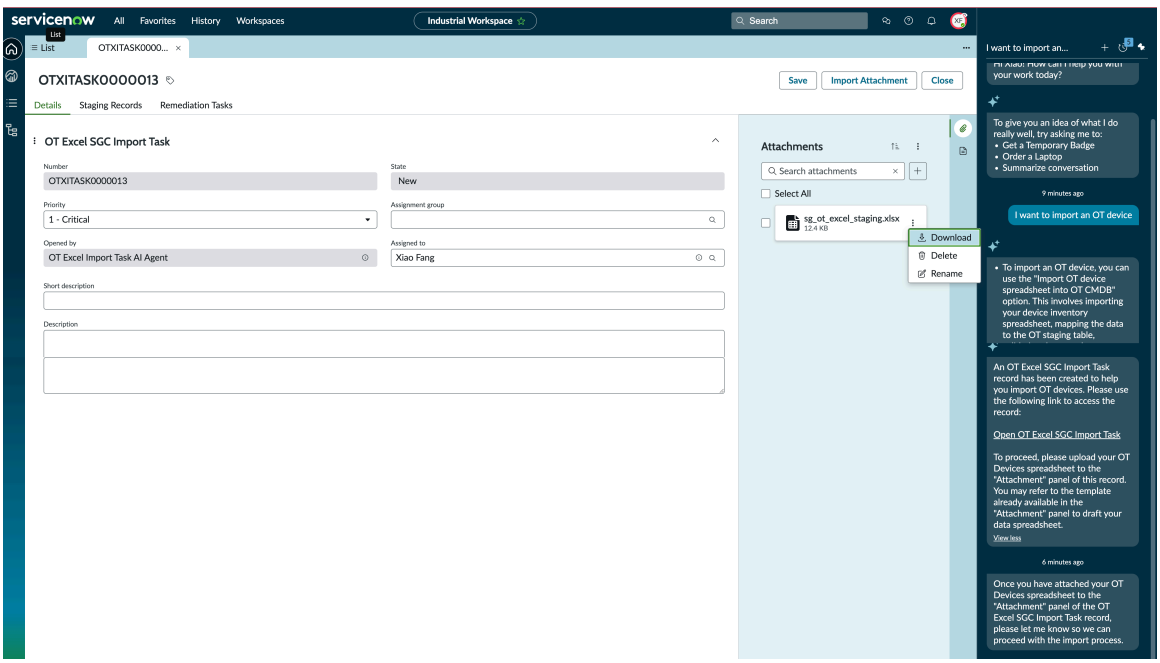
Before you begin

The ServiceNow Otto panel must be activated. For more information, see Activate the panel standard chat.

Role required: ot_excel_import_user and now_assist_panel_user

Procedure

1. Select the ServiceNow Otto icon.
   The ServiceNow Otto panel is displayed.
2. Enter a prompt such as `I want to import an OT device` to initiate the Import OT device spreadsheet into OT CMDB agentic workflow.
   The OT Excel import task AI agent begins the workflow process and creates an OT Excel SGC Import Task record. For more information about import tasks, see Using the Service Graph Connector for Microsoft Excel through import tasks.
3. Select **Open OT Excel SGC Import Task**.
4. In the Attachment panel of the import task record, download and save the Microsoft Excel spreadsheet template to your local drive.



5. After you fill out the spreadsheet with your OT device inventory, upload it in the Attachment panel.
   For more information about how to fill out the spreadsheet, see Prepare your Pre-import OT Worksheet Entry Review tool for Service Graph Connector import.
6. In the ServiceNow Otto panel, enter a prompt such as `Done` to alert the agent that you have uploaded the spreadsheet.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The agent uploads the spreadsheet to the SG OT Excel Stagings table. Wait for the **State** field of the import task record to update to **Staging import succeeded** and for the staging records to be created. You can view the staging records in the import task record's **Staging Records** tab.

7. After the import is complete, enter a prompt in the ServiceNow Otto panel, such as `Yes, proceed`.
   The prompt alerts the agent that the import was successful and can proceed to the next step. The agent validates the staging records and replies with the number of valid records, partially valid records, and invalid records. For invalid records, the agent asks whether to create a remediation task.
8. If you want to create a remediation task for the invalid records, enter `Yes`.
   The agent creates a remediation task for all invalid records so you can resolve them as needed. For more information about possible validation errors, see Managing Validations.

   The agent then asks whether to proceed importing the valid or partially invalid staging records.
9. To import the valid or partially valid staging records, enter `Yes`.
   The agent triggers the CMDB import process. The **State** field of the import task record changes to **Pending CMDB import**. After the import process is complete, the **State** field changes to **CMDB import complete**.

   The AI agent asks if you require any further assistance.
10. If no further assistance is needed, enter `No` to conclude the AI agent session.

What to do next

To verify the CMDB import, navigate to the Industrial Workspace list view and open the **All OT Devices** list. The recently imported OT device records appear in the list.

Service Graph Connector for Microsoft Excel

The Service Graph Connector for Microsoft Excel function enables you to import your existing Operational Technology data from a populated Microsoft Excel flat-file spreadsheet. You use it in the Integration Hub Extract Transform Load (ETL) to upload this data to the Configuration Management Database (CMDB).

Before you can run the import process, you must populate the Microsoft Excel spreadsheet with your existing Operational Technology data. When you import your Microsoft Excel spreadsheet using the Integration Hub ETL, it creates the correct configuration item (CI) records in the Configuration Management Database (CMDB). To learn more, see Operation Technology (OT) extension classes.

Related topics

IntegrationHub

IntegrationHub ETL

Configuring the Service Graph Connector for Microsoft Excel

Configure the Service Graph Connector for Microsoft Excel to import your existing Operational Technology data from a populated Microsoft Excel flat-file spreadsheet.

Use the Service Graph Connector for Microsoft Excel Excel guided setup and complete tasks in sequence to configure the Service Graph Connector for Microsoft Excel

Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup**, open the following guided setups, and complete the tasks.

For more information on using guided setup, see Guided Setup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign Pre-import OT Worksheet Entry Review roles

Assign roles to the users#br user groups so that you can manage the Service Graph Connector for Microsoft Excel staging table and ETL.

Before you begin

Role required: admin or user_admin

About this task

Users with the roles that are listed in the following table can use the Operational Technology Manager application.

Role	Description
OT Staging User [ot_staging_user]	Can create, edit, and view records in the staging table.
CMDB Inst Admin [cmdb_inst_admin]	Can view and edit ETL.
OT Excel Import User [ot_excel_import_user]	Can create, edit, and view Import Tasks. This is the minimum role to perform Excel SGC imports via Import Tasks. This role contains ot_staging_user.
CMDB OT Editor [cmdb_ot_editor]	Can view and reassign Excel SGC Remediation Tasks. Needs additional ot_staging_user role to perform Remediation Tasks.
CMDB OT Admin [cmdb_ot_admin]	Can perform both Import and Remediation Tasks. This role contains both ot_excel_import_user and cmdb_ot_editor.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Review class mappings

Review and update the class mappings available for the Service Graph Connector for Microsoft Excel.

Before you begin

- Ensure that the Industrial Core plugin is installed so you can view the class mapping tables available.
- Role required: admin or cmdb_ot_admin

About this task

The Service Graph Connector for Microsoft Excel uses the configuration available in the Excel SGC Class Mapping [excel_sgc_class_mapping] table to determine the best ServiceNow Configuration Management Database (CMDB) class for each configuration item (CI). You can modify these settings at any time but it is best to review the current configuration before running your first import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **OT Manager Admin** > **Excel SGC Class Mappings**.
2. Review and update the following fields in the class mapping records as needed.

Classification settings fields

Field	Description
Source Class	The class of the source CI.
Target CMDB class	The expected ServiceNow class for the CI.
OT Device type	The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example: An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is **server** and its device type is **HMI**. **Note:** In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select **No OT Function**. For OT devices where the device type is unknown, select **Unknown**.
Allow OS classification	When set to **True**, if an operating system is found on the CI, the target is switched away from the target CMDB class. The CI is assigned to a ServiceNow class that matches its OS.
Active	When checked, the class mapping is set to **Active**.

Review the system properties used by the Service Graph Connector for Microsoft Excel

As an OT Admin or CMDB Integration Admin, view system properties related to the Service Graph Connector for Microsoft Excel.

Before you begin

View a filtered list of all the system properties that are used by the Service Graph Connector.

Role required: cmdb_ot_admin or cmdb_inst_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **OT Manager Admin** > **Import OT Devices - System Properties**.
   The list shows records whose names begin with **sn_otsm_sgc.excel**.
2. Review the following system properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Service Graph Connector for Microsoft Excel system properties

System property	Description
sn_otsm_sgc.excel.fields.for.transformed.name	○ This property enables the user to provide the fields to construct the transformed name. ○ The field value or column names must be separated by comma. This transformed name is used as the name of the configuration item (CI) instead of the name field directly from the staging table. By default, the name field value is itself used as the transformed name value. ○ This property belongs to the **sn_otsm_sgc** scope and is automatically appended to this property name. ○ Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.
sn_otsm_sgc.excel.transformed.name.delimiter	○ This property specifies the delimiter to be used when computing the transformed name with more than one field or column value specified in the system property **fields.for.transformed.name**. ○ If only one column name is specified in the **fields.for.transformed.name** property, the delimiter is not used. ○ This property belongs to the **sn_otsm_sgc** scope and is automatically appended to this property name. ○ Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.
sn_otsm_sgc.excel.fields.for.validation.state.change	○ This property enables you to provide a comma-separated list of attributes so that their validation state is changed to **Pending validation**. The default value is **Empty**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System property	Description
	Note: Changes to the identifier fields, such as Mac Address, Serial Number, Transformed Name, and slot number (for OT control modules), the validation state is changed to **Pending validation**. ○ This property belongs to the sn_otsm_sgc scope and is automatically appended to this property name. ○ Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.
sn_otsm_sgc.enable.cmdb.validations	○ This property enables CMDB validations for the staging devices. If set to **True**, staging devices are validated against existing CMDB CIs for reconciliation. ○ This property belongs to the sn_otsm_sgc scope and is automatically appended to this property name. ○ Requires the admin, cmdb_ot_admin, and cmdb_inst_admin roles for read and write operations.

Add a custom field mapping in the staging table for Service Graph Connector for Microsoft Excel

With the Service Graph Connector for Microsoft Excel, add a custom field to the staging table and map the custom field to the configuration item (CI) field.

Before you begin

To configure the form layout, see Configure the form layout.

To create a custom field on the staging table, see Add and customize a field in a table.

Roles required:

- admin - Can change the script include. Can add class or field mappings and change the ETL.
- cmdb_inst_admin - Can only add new class or field mappings and change the ETL.

Procedure

1. Add custom columns to the Staging [sg_ot_excel_staging] table.
2. Navigate to **All** and in the **Filter** field, add `sg_ot_excel_staging.list`.
3. On your keyboard, press enter.
4. If needed, manually create records by selecting **New**.
5. Navigate to **All** > **Industrial Workspace Admin** > **OT Manager** > **Import OT Devices - Script Includes** and select the `SGOTAssetImportExcelConstants` script include.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. In the script, update the new column name from the staging table, and the new ETL column name inside the `SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap` object in the format “<ETL Column Name>”: “<Column Name from staging table>”.

   In this example, the “u_my_custom_field” before the colon (:) indicates the ETL column name (shown as a column in the ETL preview step), and the “u_my_custom_field” after the colon indicates the column name in the staging table.

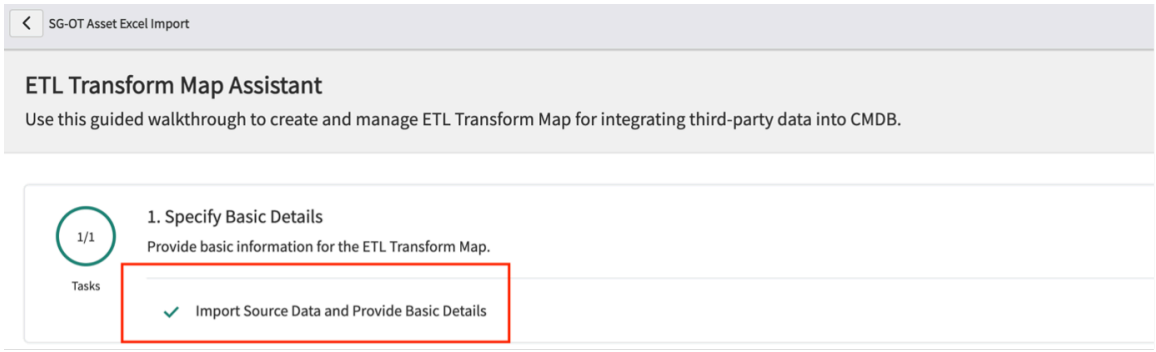
   Make sure that there’s a comma (,) added at the end of the line above the new line. In this example, a comma is added after the "custom_fields": "custom_fields" line.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

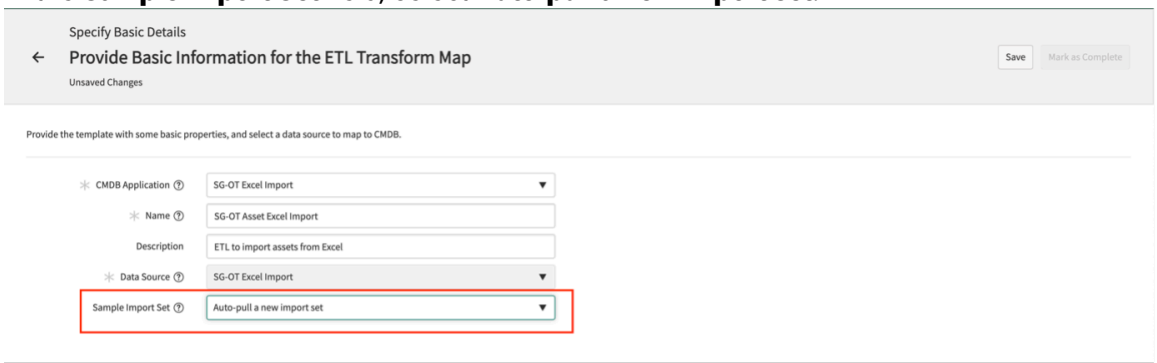
```
SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap = {
    // unique id used to uniquely identify the asset
    "id": "correlation_id",
    // Name of the asset
    "name": "transformed_name",
    // OperatingSystem of the asset
    //"operating_system": "os_version",
    // type of the asset.
    "type": "type",
    // if the asset has control module
    "has_module": "has_module",
    // id of the asset to which a control module belongs to (this is used in control module type asset).
    "control_module_parent_correlation_id": "control_module_parent_correlation_id",
    "ot_display_name": "display_name",
    "serial_number": "serial_number",
    "firmware_version": "firmware_version",
    "os_version": "os_version",
    "operating_system": "os",
    "assigned_to": "assigned_to",
    "manufacturer": "manufacturer",
    "model_number": "model_number",
    "serial_number_type": "serial_number_type",
    "purdue_level": "purdue_level",
    "asset_criticality": "asset_criticality",
    "short_description": "short_description",
    "vendor": "vendor",
    "equipment_model_entity_path": "equipment_model_entity_path",
    "first_discovered": "first_discovered",
    "hardware_version": "hardware_version",
    "status": "status",
    "backplane_name": "backplane_name",
    "backplane_id": "backplane_id",
    "slot_number": "slot_number",
    "rack_number": "rack_number",
    "module_type": "module_type",
    "device_type": "io_field_device_type",
    "support_group": "support_group",
    "site": "site",
    "ip_address": {
        "ip": "ip_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "mac_address": {
        "mac": "mac_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "memory": {
        "memory_card_serial": "memory_card_serial_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_size": "memory_size_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_type": "memory_type_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "software_installed": {
        "name": "software_installed_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "version": "software_version_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "install_date": "software_install_date_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    // Do not change this. Key should match value of SGOTAssetImportExcelConstants.CUSTOM_FIELDS_COL_NAME_IN_IMPORT_SET
    "custom_fields": {
        "customfield": "customfield_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    }
```

7. Select **Update** to save your changes.
8. Navigate to **All** > **Configuration** > **IntegrationHub ETL**.
9. Select the **CMDB Application: SG-OT Excel Import** ETL.
10. If the Invalid Mapping Data-Detected page is displayed, select **Close**.
11. From the ETL Transform Map Assistant, in the Specify Basic Details section of the guided setup, select **Import Source Data and Provide Basic Details**.

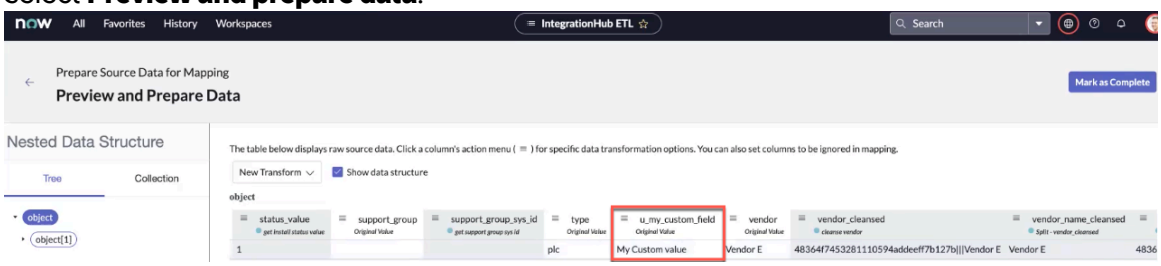
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



12. In the **Sample Import Set** field, select **Auto-pull a new import set**.



13. Select **Save**.
    The basic information saved successfully banner is displayed.
14. Select **Mark as Complete**.
15. From the ETL Transform Map Assistant page, in the Prepare Source Data for Mapping section, select **Preview and prepare data**.



    If the column isn't visible, repeat the steps 11 through 14.
16. Select **Mark as Complete**.
17. From the ETL Transform Map Assistant page, in the Map Data to CMDB and Add Relationships section, select **CMDB Classes to Map Source Data**.
18. Map the column to the target class and attribute.

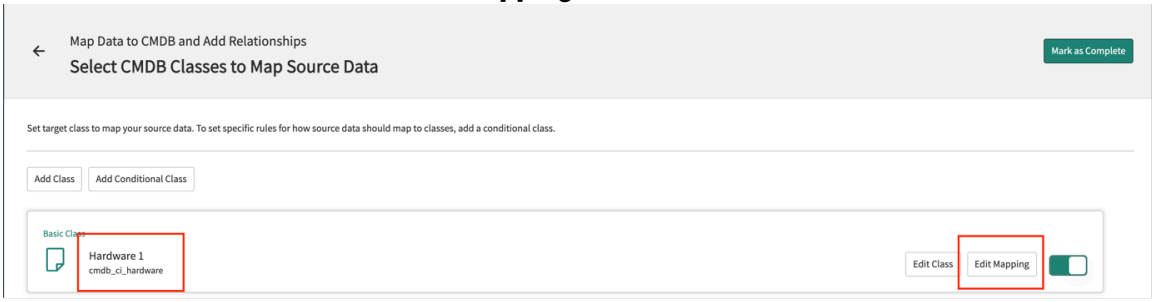
    For example, the **Comments** field is present on the Hardware [cmdb_ci_hardware] class. After the field is mapped, the **Comments** field on Hardware child classes is updated. The update occurs if the value for the Comments column in the staging table for that row isn't empty.

    If you're adding a mapping for a new field that isn't present, or for a field that isn't specific to the Hardware *cmdb_ci_hardware* class. Instead it is a field in the Operational Technology *(cmdb_ci_ot)* class, you can add the field mapping in the Operational Technology (OT) 1 stub.

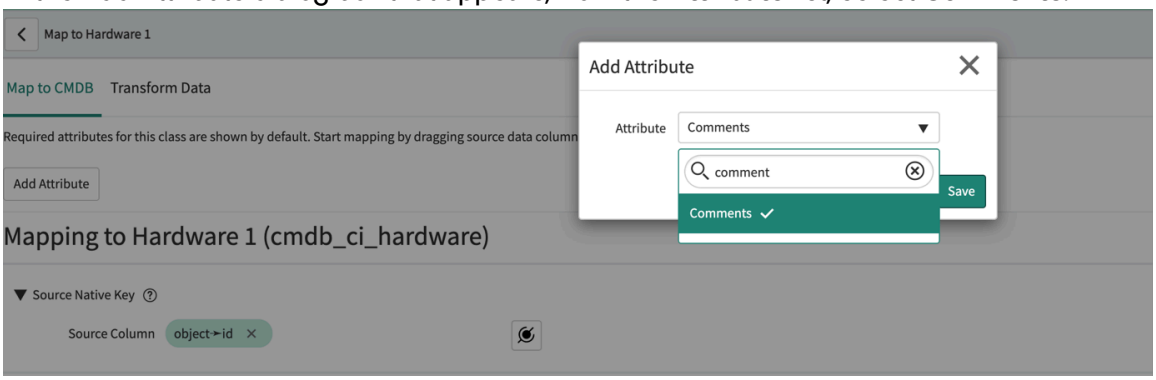
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Add a field mapping to the Hardware 1 class.

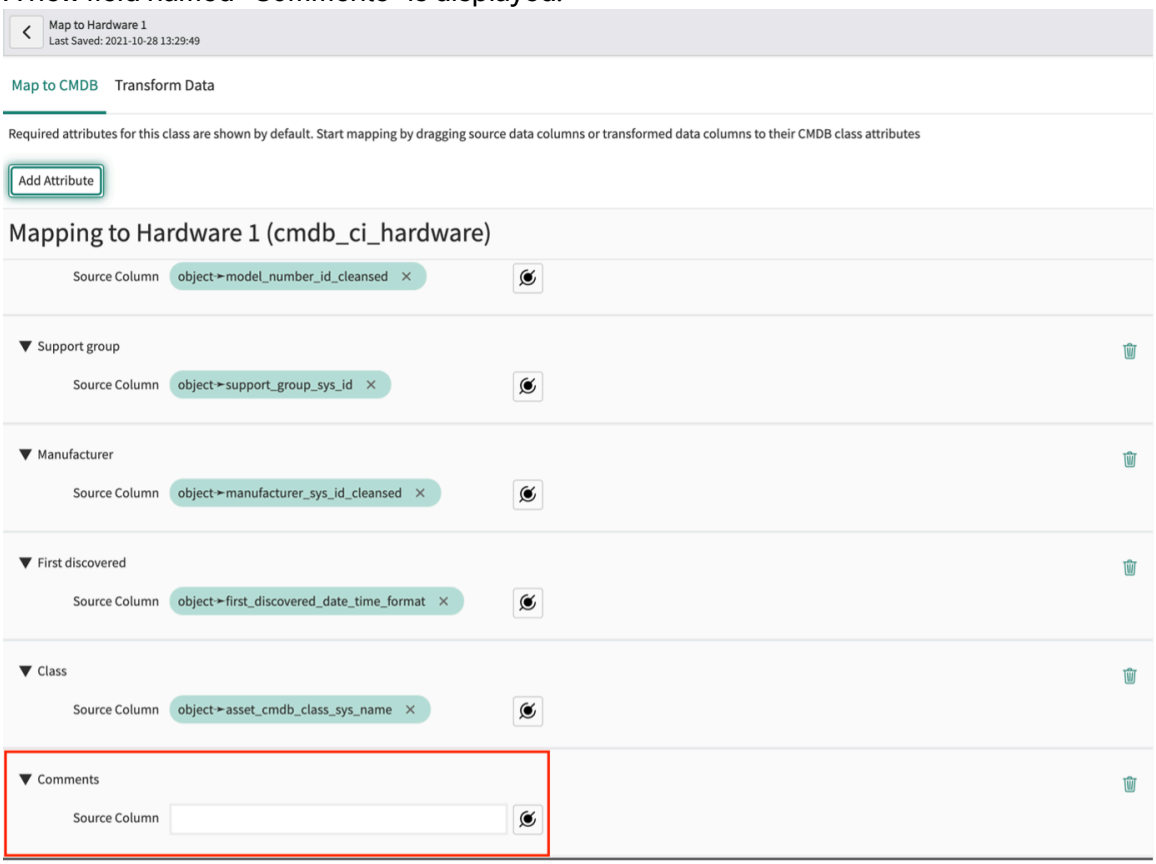
b. For the Hardware 1 class, select **Edit Mapping**.



19. In the Add Attribute dialog box that appears, from the **Attribute** list, select **Comments**.

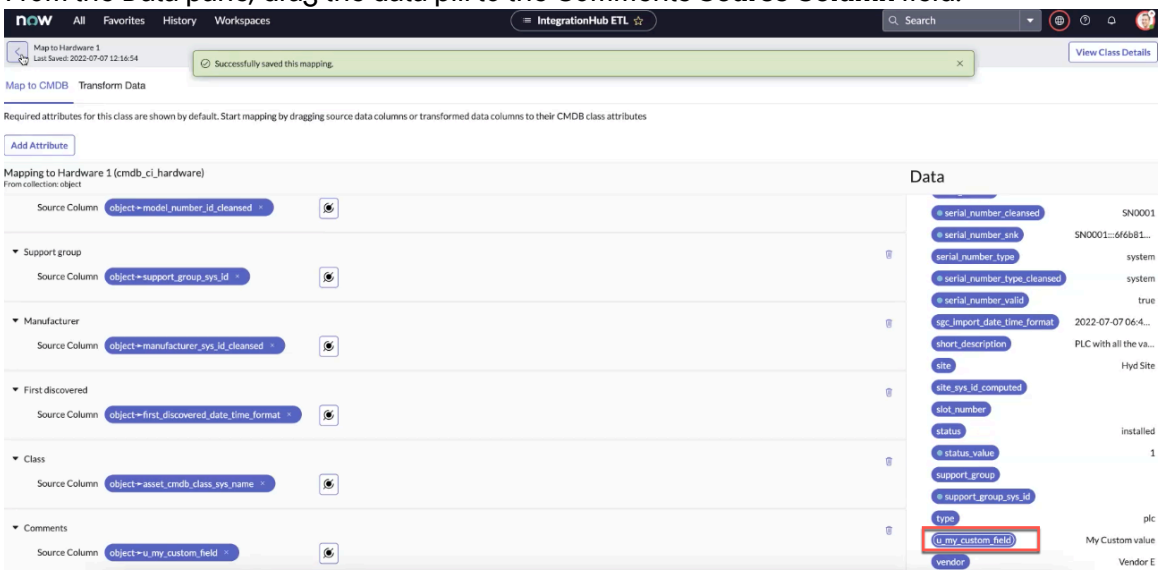


20. Select **Save**.
A new field named “Comments” is displayed.

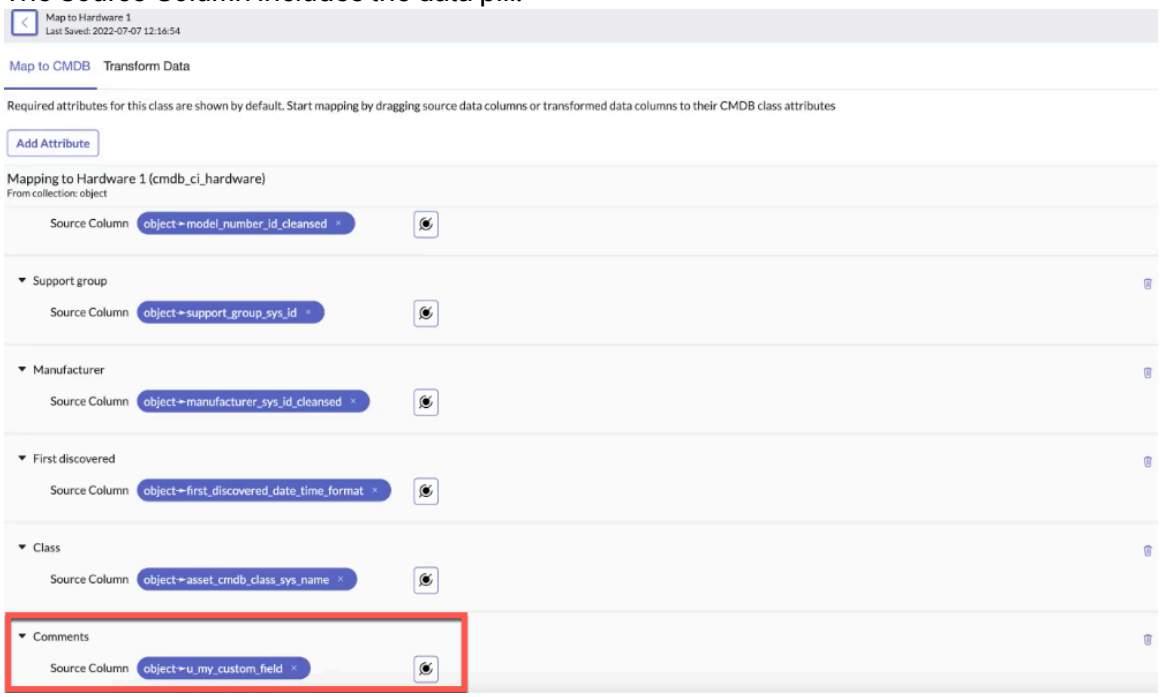


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

21. From the Data pane, drag the data pill to the Comments **Source Column** field.

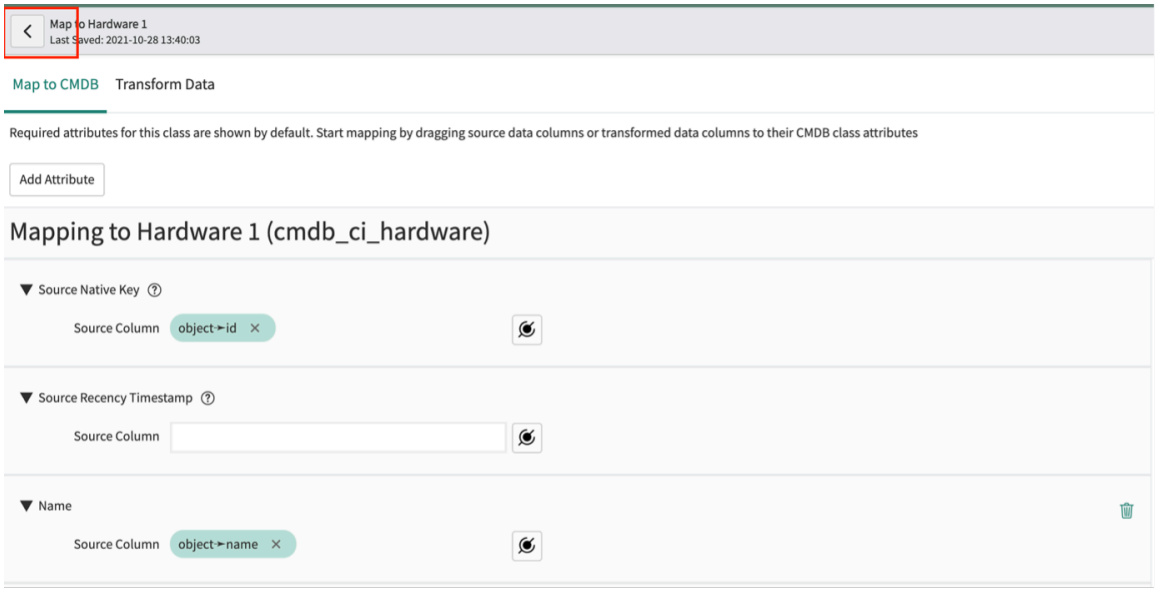


You can also select the source column icon ( ) to select the data-mapping field for it. The Source Column includes the data pill.

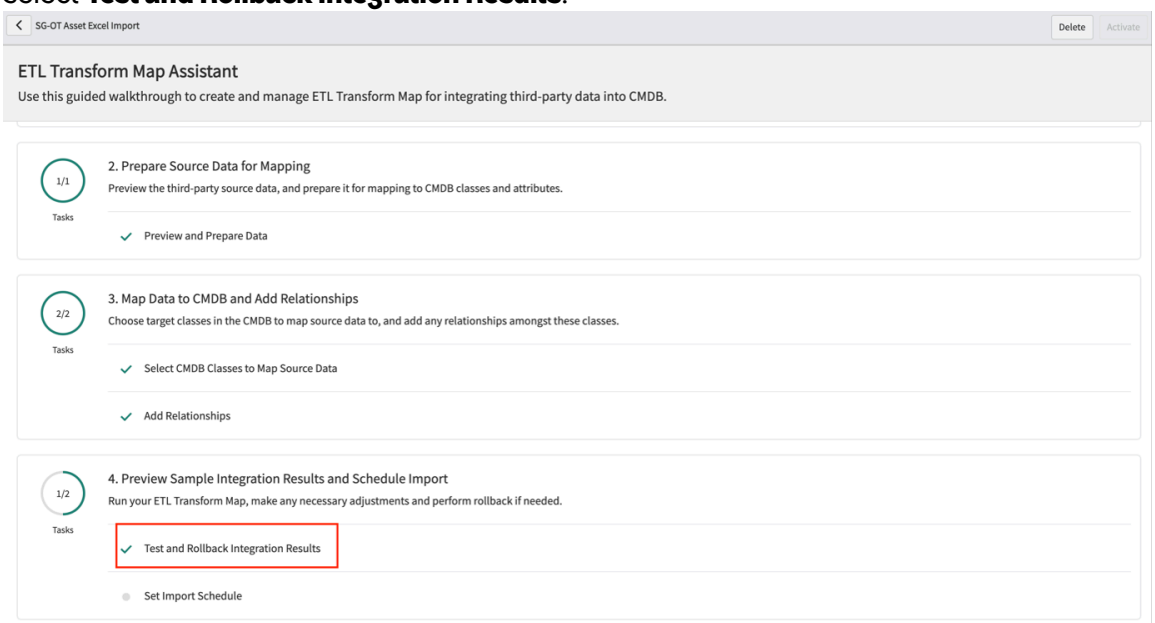


22. Navigate back to the **CMDB Classes to Map Source Data** of the Map Data to CMDB and Add Relationships section in the ETL Transform Map Assistant page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

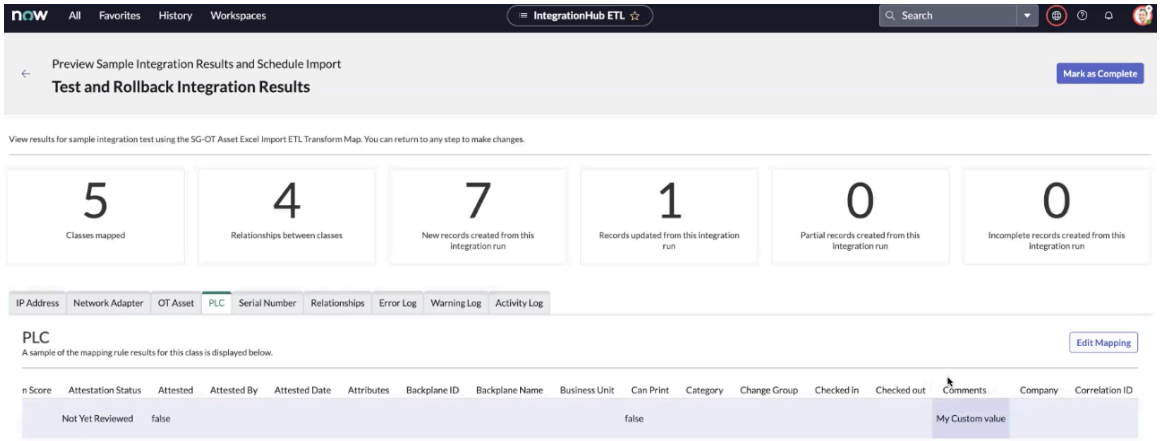


23. Select **Mark as Complete**.
24. Follow these steps to verify the new field mappings.
    a. Navigate to the home page of the ETL Transform Map Assistant.
    b. In the Preview Sample Integration Results and Schedule Import section of the guided setup, select **Test and Rollback Integration Results**.

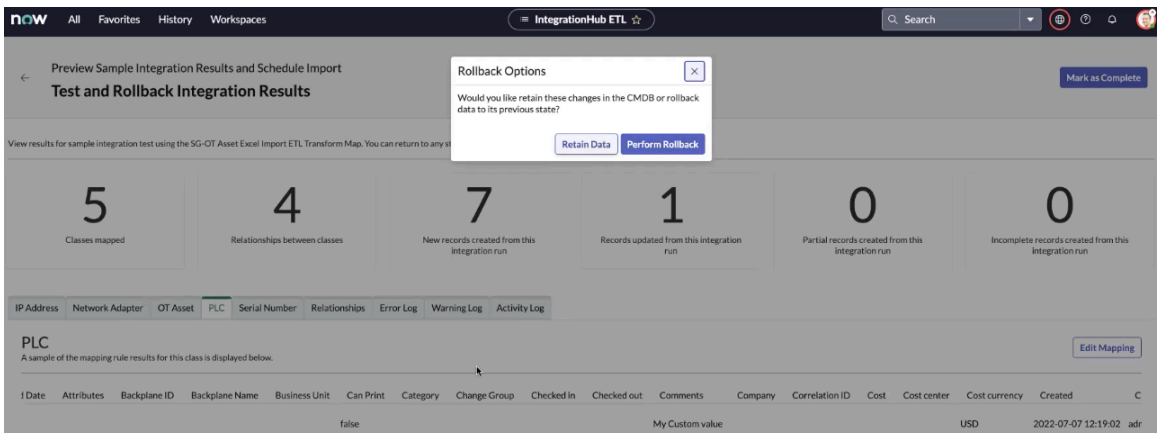


    c. Select **Run Integration**.
    d. After the run finishes successfully, confirm that the Comments field of the CI that you provided a comments value for is updated in the staging table.
    e. Select **Mark as Complete**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



f. Select **Perform Rollback**.



g. If the ETL isn't activated, select **Activate**.
The new column field mapping is successfully added and verified.

Add a custom implementation for device classification

Customize the base system classification of an device based on the type, os_version, and firmware_version.

Before you begin

The base system for the *sn_otsm_sgc.SGOTAssetImportExtensionPoint* extension point uses the default implementation script that is shipped with the name of *sn_otsm_sgc.SGOTAssetImportUtil*. To add a customized classification, create an implementation for the extension point in the **Service Graph Connector for Operational Technology (Excel)** scope.

Note: User must have only one implementation of the extension point. If you implement and activate a custom extension point rather than the default one, you must deactivate the default implementation.

Role required: admin

Procedure

1. Navigate to **All** > **System Extension Point** > **Scripted Extension points**.
2. Select *sn_otsm_sgc.SGOTAssetImportExtensionPoint*.
3. Select the **Create Implementation** related link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Enter a name for the extension point implementation.
5. In the script field, check that the class object with the following two functions is populated. Make sure that the result returned from the **getAssetCMDBSysClassNameWithOtEntityTypeSysId** extension point follows the format mentioned in the comments. Any change in the result string format results in import failure or irregularities. The format should be <cmdb class name>:::<ot entity type sys id>.

Option	Description
getAssetCMDBSysClassNameWithOtEntityTypeSysId(/*string*/ type, /*string*/ osVersion, /*string*/ firmwareVersion)	Implement this method to return the CMDB sys class name that the device belongs to, along with the OT Entity type sys_id concate nated with ":::". For unclassified devices, the OT device type is set to ot_base.
getComputerType((/*string*/ operatingSystem)	Returns the CMDB sys class name based on the operating sys tem passed.

6. After you make all the desired changes, select **Update**.
   The implementation for the extension point is created.

What to do next
From the related lists Implementations tab, open the base system extension point implementation to inactivate it.

Add a custom validation for devices

Customize the validation for your OT devices.

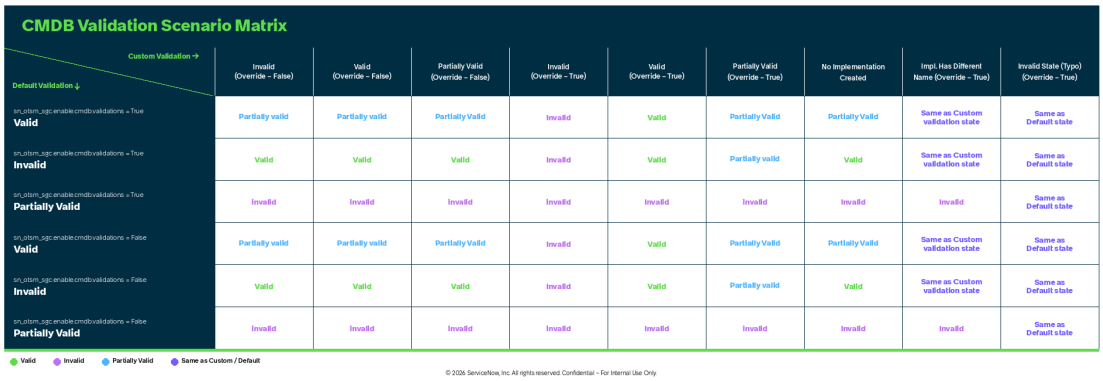
Before you begin
The base system for the **sn_otsm_sgc.SGOTAssetCustomValidationExtensionPoint** extension point uses the default **sn_otsm_sgc.SGOTExcelStagingAssetValidationProcessor** implementation script. You can add a customized validation by creating an implementation for the extension point in the Service Graph Connector for Operational Technology (Excel) scope.

Role required: admin

Procedure
1. Navigate to **All** > **System Extensions Point** > **Scripted Extension Points**.
2. Select **sn_otsm_sgc.SGOTAssetCustomValidationExtensionPoint**.
3. Select the **Create Implementation** related link.
   A script include is created where you can add your custom validation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To add a custom validation, refer to the following validation scenario.



5. Select **Update**.

Add a custom column to the staging table

Add a custom column to the SG OT Excel Stagings (sg_ot_excel_staging) table to store an additional value imported from the Microsoft Excel spreadsheet.

Before you begin

Role required: ot_excel_import_user

Procedure

1. Create a column in the SG OT Excel Staging table.
   a. Navigate to **All** > **System Definition** > **Tables**.
   b. Find and select the **SG OT Excel Staging** table record.

      Note: Use the filter conditions to help you locate the SG OT Excel Staging table record. For example, you can set a filter of **[Label] [contains] [SG OT Excel]**.

   c. On the **Columns** tab, select **New**.
   d. In the **Type** field, select **String**.
   e. In the **Column label** field, enter a label for the new column.
      The **Column name** field value is generated from the column label.
   f. In the **Max length** field, enter the maximum number of characters for the column.

      For example, `100`.

   g. Select **Submit**.

   After refreshing the SG OT Excel Staging table record, the new column appears under the **Columns** tab.
2. Add the column to the SG OT Excel Stagings list view.
   a. Open the **SG OT Excel Stagings** table by navigating to **All**.
   b. In the **Filter** field, add `sg_ot_excel_staging.list` then press the Enter key.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Select the **Personalize List** icon.

d. Under **Available**, locate and select the column you created.

e. Use the **Add** arrow to add the column to **Selected**.

f. Select **OK**.

Result
The column you created is now available in the SG OT Excel Stagings table.

What to do next
Add a matching column to the SG-OT Excel Staging Import [sn_otsm_sgc_sg_ot_excel_pre_import] table so the imported value has a source field to map from. For more information, see Add a matching column to the pre-import table.

Add a matching column to the pre-import table

Add a column to the SG-OT Excel Pre Import table that matches the custom column on the staging table, giving the imported value a source field for mapping.

Before you begin
A custom column must be added to the staging table before completing this task. For more information, see Add a custom column to the staging table.

Role required: ot_excel_import_user

Procedure
1. Navigate to **All** > **System Definition** > **Tables**.
2. Find and select the **SG-OT Excel Pre Import** table record.

   Note: Use the filter conditions to help you locate the SG-OT Excel Pre Import table record. For example, you can set a filter of **[Label] [contains] [SG-OT Excel]**.

3. On the **Columns** tab, select **New**.
4. In the **Type** field, select **String**.
5. In the **Column label** and **Max length** fields, enter the same label for the column you added in the SG OT Excel Staging table.
   The **Column name** field value is generated from the column label.
6. Select **Submit**.

What to do next
Map the source field on the pre-import table to the target field on the staging table in the table transform map. For more information, see Map the custom field in the transform map.

Map the custom field in the transform map

Map the custom source field on the pre-import table to the target field on the staging table so the imported value transforms into the correct staging column.

Before you begin
The custom column must be added to both the staging table and the pre-import table before completing this task. For more information, see Add a custom column to the staging table and Add a matching column to the pre-import table.

Role required: ot_excel_import_user

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **OT Manager Admin** > **Import OT Devices - Data Sources**.
2. Select the **SG OT Excel Staging Import** record.
3. Under the **Transforms** tab, select the sn_otsm_sgc_sg_ot_excel_pre_import transform map record.
4. Under the **Field Maps** tab, select **New**.
5. Set the **Source field** value to the same column you created in the SG-OT Excel Pre Import Staging table.
6. Set the **Target** value to the same column you created in the SG OT Excel Stagings [sg_ot_excel_staging] table.
7. Select **Submit**.

Result
The field map is added to the SG-OT Excel Pre Import [sn_otsm_sgc_sg_ot_excel_pre_import] table transform map record.

What to do next
Complete the custom column import by uploading a Microsoft Excel spreadsheet with the custom column data. For more information, see Complete the custom column import.

Complete the custom column import

Upload an updated Microsoft Excel spreadsheet to populate the custom column and complete the import.

Before you begin
Role required: ot_excel_import_user

Procedure

1. Create a record in the OT Excel SGC Import Task table.
2. From the record, download the attached **sg_ot_excel_staging.xlsx** file.
3. In the Microsoft Excel file, add your custom column and fill in the data for your configuration item (CI) records.
4. Upload the updated Excel file to the OT Excel SGC Import Task record.
   For more information about completing the custom column import with an import task and validating the imported staging records, see Create an import task and Validate imported staging records.

What to do next
Update the column mapping script with the custom column. For more information, see Update the column mapping script.

Update the column mapping script

To transfer the custom column data to the Configuration Management Database (CMDB), update the column mapping script to add the corresponding entry to the **importSetColumnsVsStagingColumnsMap** object.

Before you begin
Role required: ot_excel_import_user

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The **importSetColumnsVsStagingColumnsMap** object in the **SGOTAssetImportExcelConstants** script controls which columns from the SG OT Excel Stagings (sg_ot_excel_staging) table are included when you trigger the CMDB import process. If you add a custom column to the staging table, you must add a corresponding entry to the **importSetColumnsVsStagingColumnsMap** object. Otherwise, the custom column is ignored during import. For more information about triggering the CMDB import process, see Trigger a CMDB import for valid staging records.

Each entry in **importSetColumnsVsStagingColumnsMap** object is a key-value pair with the following format:

```
"<import set column name>": "<staging table column name>"
```

The key is the field name that appears in the JSON payload sent to the CMDB import (sn_otsm_sgc_sg_ot_excel_import) set. The value is the name of the corresponding column on the SG OT Excel Stagings table.

When you create a key and value, they're typically identical. For example, a custom staging column named **u_my_custom_field** maps to itself. Only use a different name if you need the import set field name to differ from the staging table column name.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Import OT Devices - Script Includes**.
2. Select the **SGOTAssetImportExcelConstants** record.
3. In the **importSetColumnsVsStagingColumnsMap** object, add a line in the following format:
   `"ETL Column Name": "Staging Table Column Name"`

   For example: `"u_my_custom_field": "u_my_custom_field"`
4. Before your new entry, add a comma at the end of the line so that the object remains valid JavaScript.
5. Select **Update**.

What to do next

Configure the Robust Transform Engine (RTE) mapping for the Extract Transform Load (ETL). For more information, see Configure the RTE mapping for ETL.

Configure the RTE mapping for ETL

Configure the Robust Transform Engine (RTE) mapping for the Extract Transform Load (ETL). The ETL process transfers custom column data from the import set to the target Configuration Management Database (CMDB) class.

Before you begin

- Complete the update for the column mapping script. The custom column must be included in the JSON file exported to the import set before the RTE can map it. For more information, see Update the column mapping script.
- Role required: admin

About this task

When you select the **Trigger CMDB Import** UI action, the exported staging records are loaded into the SG-OT Asset Excel Import set and processed through the following RTE entities:

Import

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The raw field on the import set record (the JSON key produced by importSetColumnsVsStagingColumnsMap).

temp

An intermediate staging entity used to hold the value during transformation.

CI class stub

The target field on the CMDB CI class that stores the value.

The data is processed from the Import to the temp to the CI class stub. You must define a field for each entity the data passes through and map each pair of entities.

Warning: Use the same column name in the RTE entity fields as the key you used in the **importSetColumnsVsStagingColumnsMap** object. Using different names results in the RTE not finding the data to transform.

For more information about triggering the CMDB import process, see Trigger a CMDB import for valid staging records.

Procedure

1. Create a field for the Import entity.
   a. Select **All**.
   b. In the **Filter** field, enter `sys_rte_eb_field.do` to open a new record form in the RTE Entity Field (sys_rte_eb_field) table.
   c. In the **Name** and **Field/Path** fields, enter the name of your custom column.
   d. Set the **Entity** field to **Import**.
   e. Set the **Definition** field to **SG-OT Asset Excel Import**.
   f. Select **Submit**.
2. Create a field for the temp entity.
   a. Select **All**.
   b. In the **Filter** field, enter `sys_rte_eb_field.do` to open a new record form in the RTE Entity Field (sys_rte_eb_field) table.
   c. In the **Name** and **Field/Path** fields, enter the name of your custom column.
   d. Set the **Entity** field to **temp**.
   e. Set the **Definition** field to **SG-OT Asset Excel Import**.
   f. Select **Submit**.
3. **Optional:** Create a field for the configuration item (CI) class entity.

   Note: Only complete this step if the custom field is being added to the target CMDB CI class.

   a. Select **All**.
   b. In the **Filter** field, enter `sys_rte_eb_field.do` to open a new record form in the RTE Entity Field (sys_rte_eb_field) table.
   c. In the **Name** and **Field/Path** fields, enter the name of your custom column.
   d. Set the **Entity** field to the CMDB class stub you want to target.
   e. Set the **Definition** field to **SG-OT Asset Excel Import**.
   f. Select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Create a mapping from Import to temp.

   a. Select **All**.

   b. In the **Filter** field, enter `sys_rte_eb_field_mapping.do` to open a new record form in the RTE Entity Field Mapping (sys_rte_eb_field_mapping) table.

   c. Set the **Source** to the custom column from the Import entity.

   d. Set the **Target Field** field to the custom column from the temp entity.

   e. In the **Order** field, enter any value.
   For example, `100`.

   f. Set the **Entity Mapping** field to `impTotemp`.

   g. Set the **Definition** field to **SG-OT Asset Excel Import**.

   h. Select **Submit**.

5. Create a mapping from temp to the CMDB class stub.

   a. Select **All**.

   b. In the **Filter** field, enter `sys_rte_eb_field_mapping.do` to open a new record form in the RTE Entity Field Mapping (sys_rte_eb_field_mapping) table.

   c. Set the **Source** to the custom column from the temp entity.

   d. Set the **Target Field** field to the matching column from the target CMDB class entity stub.

   e. In the **Order** field, enter any value.
   For example, `100`.

   f. Set the **Entity Mapping** field to `tempTo` followed by the CMDB class you're targeting.

   g. Set the **Definition** field to **SG-OT Asset Excel Import**.

   h. Select **Submit**.

Result

After you configure these mappings, the custom column data populates correctly in the CMDB when you select the **Trigger CMDB Import** UI action.

Testing the Service Graph Connector for Microsoft Excel

These troubleshooting actions can help resolve common issues when importing your Operational Technology devices or data. Access the System Log to troubleshoot for these errors.

These logs can be used to debug any issues or to find the Service Graph Connector steps are executed properly.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Issue	Solution
If there are entries in the Partial payload tab after test running the Service Graph Connector from ETL Guided Setup	Due to the following conditions: • Missing values for the required fields of an device. • Control Modules without a parent device associated with it - Check that the type of the device and control module parent id field is filled properly in the staging table.
If there are entries in the Incomplete payload tab after test running the Service Graph Connector from the ETL Guided Setup	Due to the missing values for fields that are used uniquely to identify an device.
If the timestamp column appears empty on the staging table	The user must use the UTC format (YYYY-MM-DD hh:mm:ss) to enter the date and time.
If the validation state update on records isn't visible after the validation process	The user must manually refresh the page.
When the user changes the existing data of the records in the staging table, the validation state is not set to Pending Validation.	The validation state is set to Pending validation, when the following attributes are changed: • Identifier fields (Mac-address (1-9)) • Serial Number • Name • Correlation ID • Type • Control module parent correlation ID • Fields used in transformed name computation • Rack Number • Slot Number For more information about the system properties, see Review the system properties used by the Service Graph Connector for Microsoft Excel.
After records are imported into the staging table, the updates done in the system properties related to transformed name computation are not reflected in the staging table records.	Change the system properties before importing the data into the staging table.
If the duplicate records exist in CMDB, the staging table does not detect it as duplicate.	The validations are executed only for the data available in the staging table. The validations are not executed for the data available in the CMDB.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Issue	Solution
The site name is provided in the spreadsheet or staging table but isn't shown on the OT devices after the import of the spreadsheet.	Only the existing site records in the CMDB are considered. The entity_name for the site (ISA Equipment model entity) must match the value provided in the site column in the excel or staging table. If the entity_name for the site does not match, the value is set to empty.

View script includes used by the Service Graph Connector for Microsoft Excel

As an admin, view the script includes related to the Service Graph Connector for Microsoft Excel

Before you begin

View a filtered list of all the scripts that are used by the Service Graph Connector for Microsoft Excel.

Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **OT Manager** > **Import OT Devices - Script Includes**.
   This list shows the records whose names begin with SGOTAsset or SGOTExcelStaging.
2. View the list of scripts.

Using the Service Graph Connector for Microsoft Excel through import tasks

With the Service Graph Connector for Microsoft Excel, you can create import tasks that handle the upload, validation, and import of staging records for your OT device data into the Configuration Management Database (CMDB).

Import task overview

Users assigned the OT Excel Import User [ot_excel_import_user] role can create import tasks in the Industrial Workspace. Import tasks handle the following tasks.

- Upload the populated Microsoft Excel spreadsheet into staging table.
- Validate the staging records created from the Microsoft Excel spreadsheet.
- Import the valid staging records into the CMDB.
- Optionally, create remediation tasks for invalid staging records.

Create an import task

Create an import task for the Service Graph Connector for Microsoft Excel to handle the import of Operational Technology (OT) device data from your Microsoft Excel spreadsheet.

Before you begin

Role required: ot_excel_import_user

About this task

Watch this short video to learn how to create an import task in the Industrial Workspace.

https://player.vimeo.com/video/1125340822?h=55052711fc&badge=0&autopause=0&player_id=0&app_id=58479

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the Industrial Workspace, select the **List** () icon.
2. Under the OT Excel SGC - Import Task module, select one of the available lists.
3. Select **New**.
4. On the form, fill in fields.
5. Select **Save**.
6. Refresh the form to access the Microsoft Excel template.
7. From the **Attachments** panel, download the Microsoft Excel template by selecting the **Actions**  icon next to the **sg_ot_excel_staging.xlsx** template and clicking **Download**.
8. Save the template locally on your computer.
9. Fill in the template as needed with your OT device data.
   For more information about how to fill out the spreadsheet, see Prepare your Pre-import OT Worksheet Entry Review tool for Service Graph Connector import.
10. From the **Attachments** panel, delete the original template by selecting the **Actions** icon next to the **sg_ot_excel_staging.xlsx** and clicking **Delete**.
11. Upload your completed Microsoft Excel spreadsheet.

    a. Ensure that you are assigned to the import task so that you can see the **Import Attachment** UI action.
    If you are not in the **Assigned to** field of the import task, click the **Assign to me** UI action before proceeding with the next step.

    b. Click **Select file**.

    c. From your local drive, upload the completed Microsoft Excel spreadsheet.

    d. Once the spreadsheet is updated, select the **Import Attachment** UI action.

    e. Wait for your system to complete the import process.
    Once complete, the **State** field changes from **Pending staging import** to **Staging import succeeded**.

Result
After the import process is complete and the Microsoft Excel spreadsheet has been successfully imported, select the **Staging Records** tab to view the staging records for your Operational Technology (OT) device data.

What to do next
After the import process is complete, you can validate the imported staging records. For more information, see Validate imported staging records.

Prepare your Pre-import OT Worksheet Entry Review tool for Service Graph Connector import

Prepare your spreadsheet by positioning your existing data in the correct columns is crucial to the success of your upload.

Before you begin
Role required: ot_excel_import_user

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Procedure

1. Fill the following columns in the Microsoft Excel spreadsheet.

   Note: Column names cannot be changed. Extra columns can be added to the staging table.

   For more information about adding a new custom field mapping in the staging table, see Add a custom field mapping in the staging table for Service Graph Connector for Microsoft Excel. For more information about adding a custom column to the staging table, see Add a custom column to the staging table.

   .

Refer to the following tables for guidance while filling in the spreadsheet. The spreadsheet contains many columns. The examples and field descriptions are split into multiple sections.

- Filling in columns A through K
- Filling in columns L through Y
- Filling in columns Z through AI
- Filling in columns AJ through AT
- Filling in columns AU through BD
- Filling in columns BE through BR
- Filling in columns BS to BW
- Filling in columns 1 to 8

Columns A through K

Column	Required column name	Type	Description and example
A	Device criticality	string	Measure of how critical, or important, the OT device is, based on its role. Examples: ○ High or Most critical ○ Medium or somewhat critical ○ Low or Less critical ○ None or not critical
B	Assigned to	string	Email address of the user that this OT device is assigned to. For example: bob@example.com
C	Backplane id	string	Unique ID that is used for the identification of the backplane and mapping to control modules. For example: BPSN123
D	Backplane name	string	Name of the backplane, if any, for the OT device. Examples: Backplane #51, PLC1 Backplane
E	Control module parent id	string	Unique ID that is used for the identification of the control modules to the parent control system backplane. For example: 482bb239-05e8-4bad-ba59-925eb87ff06e

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
F	Correlation id	string	Unique ID that is used for identification of the OT device. Enter the correlation_id a string. Examples: 482bb239-05e8-4bad-ba59-925eb87ff06e or 5123456. This column entry is required. ○ Each imported OT device must have a correlation_id that is unique. ○ The OT device data that you import normally originates in an external source system, which usually assigns a unique identifier to each record.
G	Custom field 1	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes. Examples: Refurbished, Used
H	Custom field 2	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes. Examples: Painting, Stamping
I	Custom field 3	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes.
J	Custom field 4	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes.
K	Custom field 5	string	(Optional) Custom data for the OT device is stored in the Attributes field on the CI. You can use this column to associate free-form data to the OT device for categorization or other purposes.

Columns L through Y

Column	Required column name	Type	Description and example
L	Display name	string	Used to populate the display name of OT devices.
M	Equipment model entity path	string	Path of the equipment model entity that the OT device is mapped to.
N	Firmware version	string	Firmware version of the OT device, if any. For example: 12.0

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
O	First discovered	datetime	ISO-formatted timestamp of the first time that the OT device was first discovered on your network. For example: YYYY-MM-DD HH:MM:SS.
P	Hardware version	string	Hardware version of the OT device, if any. For example: 13.2
Q	Has module	Boolean	For control systems with modules, indicates that this system has modules. Examples: True, False
R	IO field device type	string	If this device is a field device, indicates if it is used for input, output, or both. Examples: ○ input ○ output ○ input_output The device acts as both input and output.
S	IP Address 1	string	First IP address, if any, that is associated with the OT device. If there are multiple IP addresses, use the next IP address column (IP Address 2). Examples: 10.0.0.22, 10.0.0.12
T	IP Address 2	string	Second IP address, if any, that is associated with the OT device. Examples: 192.168.100.1, 192.168.100.5
U	IP Address 3	string	Third IP address, if any, that is

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			associated with the OT device.
V	IP Address 4	string	Fourth IP address, if any, that is associated with the OT device.
W	IP Address 5	string	Fifth IP address, if any, that is associated with the OT device.
X	IP Address 6	string	Sixth IP address, if any, that is associated with the OT device.
Y	IP Address 7	string	Seventh IP address, if any, that is associated with the OT device.

Columns Z through AI

Column	Required column name	Type	Description and example
Z	IP Address 8	string	Eighth IP address, if any, that is associated with the OT device.
AA	IP Address 9	string	Ninth IP address, if any, that is associated with the OT device.
AB	MAC Address 1	string	First MAC address, if any, that is associated with the OT device. If there are multiple MAC addresses, use the next Mac address column (MAC Address 2). Examples: 94:94:1d:01:6d:5f, cc:7c:4a:fb:20:71

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Note: For an OT device, you must create an entry in at least one of these three spreadsheet columns, all values in these columns must be unique for the spreadsheet: ○ MAC Address 1 ○ Name ○ Serial number
AC	MAC Address 2	string	Second MAC address, if any, that is associated with the OT device. For example: e5:4d:c8:36:b1:2d
AD	MAC Address 3	string	Third MAC address, if any, that is associated with the OT device.
AE	MAC Address 4	string	Fourth MAC address, if any, that is associated with the OT device.
AF	MAC Address 5	string	Fifth MAC address, if any, that is associated with the OT device.
AG	MAC Address 6	string	Sixth MAC address, if any, that is associated with the OT device.
AH	MAC Address 7	string	Seventh MAC address, if any, that is associated with the OT device.
AI	MAC Address 8	string	Eighth MAC address, if any, that is associated with the OT device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Columns AJ through AT

Column	Required column name	Type	Description and example
AJ	MAC Address 9	string	Ninth MAC address, if any, that is associated with the OT device.
AK	Manufacturer	string	Name of the manufacturer of the OT device. Examples: Rockwell Automation, Dell
AL	Memory card serial 1	string	Assigned serial number of the first memory card, if any, that is installed in the OT device. If there are multiple memory cards, use the next memory card serial column (Memory card serial 2). Examples: MMC DA362131, MemSN123
AM	Memory card serial 2	string	Assigned serial number of the second memory card, if any, that is installed in the OT device. For example: MemSN123
AN	Memory card serial 3	string	Assigned serial number of the third memory card, if any, that is installed in the OT device.
AO	Memory size 1	string	Size of the first memory card, if any, that is installed in the OT device. Examples: 256 GB or 1 GB
AP	Memory size 2	string	Size of the second memory card, if any, that is installed in the OT device. Examples: 256 GB or 1 GB
AQ	Memory size 3	string	Size of the third memory card, if any, that is installed in the OT device. Examples: 256 GB or 1 GB
AR	Memory type 1	string	Type of memory card that is installed in the OT device. If there are multiple memory cards, use multiple columns. For example: RAM
AS	Memory type 2	string	Type of memory card that is installed in the OT device. Examples: RAM
AT	Memory type 3	string	Type of memory card that is installed in the OT device.

Columns AU through BD

Column	Required column name	Type	Description and example
AU	Model number	string	Manufacturer's model number for the OT device. Examples: ThinkServer TD230, XPS 15z
AV	Module type	string	Description of the function of the control module, if this device is one. Examples: Input, Output
AW	Name	string	Host name of the OT device, usually as part of the FQDN. Examples: PLC1, Door Assembly HMI, and Robot Control Module.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Note: For an OT device, you must create an entry in at least one of these three spreadsheet columns. All values in these columns must be unique for the spreadsheet: ○ MAC Address 1 ○ Name ○ Serial number
AX	Operating system	string	Operating system, if any, that is installed on the OT device. Examples: Linux Fedora, Windows 10, Windows 2000, Mac OS 8. **Note:** For an OT device, you should create entries in the following spreadsheet columns, even though they are not required: ○ Type ○ If available, Operating System ○ If available, Firmware version
AY	OS version	string	Reported version of the operating system, if any, that is installed on the OT device. Examples: 10.0, 13.5.2 **Note:** For an OT device, you should create entries in the following spreadsheet columns, even though they are not required: ○ type ○ If available, os_version ○ If available, firmware version
AZ	OT Staging Task	string	Tasks created to remediate invalid records on the staging table.
BA	Purdue level	string	Assigned Purdue level for the OT device. Assigning a Purdue level ensures that the Discovery for the Operational Technology function properly locates each item at the correct ICS level and produces accurate Discovery results. Examples: 1, 2, 3
BB	Rack number	string	Rack where the control module is mounted. Examples: 1, 2, 3
BC	Serial number	string	Assigned serial number, if any, for the OT device. Examples: SN545, SN998

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Note: For an OT device, you must create an entry in at least one of these three spreadsheet columns. All values in these columns must be unique for the spreadsheet: ○ MAC Address 1 ○ Name ○ Serial number
BD	Serial number type	string	Normally set to the value of "system," but it could be a different type of serial number. For example: uuid

Columns BE through BR

Column	Required column name	Type	Description and example
BE	Short description	string	Short description of the OT device. Examples: HMI for the Door Painting Cell, Controls the door assembly robot.
BF	Site	string	The equipment models start at the site level and contain a detailed hierarchical structure that describes each industrial site. For more information, see ISA-95 equipment model.
BG	Slot number	string	For a control module, indicates the slots that this device occupies in the chassis of the control system. Examples: 1, 2
BH	Software install date 1	datetime	Date that the application software was installed on the OT device. If there are multiple dates, use multiple columns. Use only UTC format for the date. For example: YYYY-MM-DD HH:MM:SS
BI	Software install date 2	datetime	Date that the application software was installed on the OT device. If there are multiple dates, use multiple columns. Use only UTC format for the date. For example: YYYY-MM-DD HH:MM:SS
BJ	Software install date 3	datetime	Date that the application software was installed on the OT device. If there are multiple dates, use multiple columns. Use only UTC format for the date. Example: YYYY-MM-DD HH:MM:SS.
BK	Software installed 1	string	Name of the application software, if any, that is installed on the OT device. If there are multiple names, use multiple columns. For example: Rockwell HMI Vision

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
BL	Software installed 2	string	Name of the application software, if any, that is installed on the OT device.
BM	Software installed 3	string	Name of the application software, if any, that is installed on the OT device.
BN	Software version 1	string	Reported version of the application software, if any, that is installed on the OT device. If there are multiple versions, use multiple columns. For example: v1.2 or v2011 SP3 HF2 or 4.54.32145
BO	Software version 2	string	Reported version of the application software, if any, that is installed on the OT device. For example: v1.2 or v2011 SP3 HF2 or 4.54.32145
BP	Software version 3	string	Reported version of the application software, if any, that is installed on the OT device. For example: v1.2 or v2011 SP3 HF2 or 4.54.32145
BQ	Status	string	Status of the OT device: **--None--** No assigned status. **Absent** OT device is absent in your facilities. **In Maintenance** OT device is in maintenance and currently is off line. **In stock** OT device is in stock in your facilities. **Installed** OT device is installed in your facilities. **Pending Install** OT device is pending installation in your facilities. **Pending repair** OT device is pending repair but is not online yet. **Retired** OT device is retired. **Stolen** OT device has been stolen.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Note: The values in this field are mapped to **Life Cycle Stage** and **Life Cycle Stage Status** fields on the CI form.
BR	Support group	string	Name of the primary support group for this OT device. Examples: Door Support, Corporate IT Support.

Columns BS to BW

Column	Required column name	Type	Description and example
BS	Transformed name	string	Users must not fill this column. By default, the transformed name value is populated using transformed column system properties. A user cannot edit the Transformed name. For system properties, see Review the system properties used by the Service Graph Connector for Microsoft Excel.
BT	Type	string	Type of OT device/ configuration item (CI). Examples: PLC, DCS

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Note: ○ For a listing and explanation of valid CI types, see Operation Technology (OT) extension classes. ○ For an OT device, you should create entries in the following spreadsheet columns, even though they are not required: ▪ type ▪ os_version
BU	Validation comments	string	Users must not fill this column. By default, Validation comments are populated after the validations are run on the staging table records that are imported from excel. Validation comments are not updated when records are imported. User cannot edit the Validation comments.
BV	Validation state	string	Users must not fill this column. By default, the validation state is populated when the data is imported in the staging table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Status of the OT device: **Pending validation** Default state when records are imported into the staging table. **Invalid** Cannot uniquely create a CI record in the CMDB. **Partially valid** One of the Transformed Name, MAC Address 1, and Serial number has no value. All the other fields (correlation id, control module parent id) have values. **Valid** All identifiers are present and are ready for import.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Description and example
			Imported Completed the import of the data from the staging table to the Import set table. User cannot edit the Validation state.
BW	Vendor	string	Name of the vendor of the OT device.

Columns 1 to 8

Column	Required column name	Type	Choice columns if applicable	Description and example
1	Backup configuration status	choice list	Backup Enabled, Backup Disabled, Unknown, Not Applicable, Planned, Not Planned	Indicates whether the CI has been configured in the backup service or appliance with relevant policies. Examples: Backup Enabled
2	Backup execution mode	choice list	Manual, Automatic, Manual or Automatic, Unknown	Indicates whether the backup is configured to run automatically on a periodic basis, or if it is manually executed on an as-needed basis. Examples: Manual, Automatic
3	Backup source id	string		Backup service source identifier for a device, which identifies the device in external or

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Choice columns if applicable	Description and example
				internal backup services. Backup source id can include host_id, vcenter_id, instance_id, db_id. Examples: AdvWrks2008R2Backup
4	Last backup attempt	glide_date_time		Date and time of the last backup attempt made for a device. Examples: 2024-06-18 09:53:37
5	Last successful backup	glide_date_time		Date and time of the last successful backup made for a device. Examples: 2024-06-18 09:53:37
6	Backup recovery point objective	glide_duration		Represents the amount of time that can elapse between backups and the amount of data lost. Examples: 90 12:00:00
7	Backup managed by	string		Email ID of the user responsible for managing the backup. Examples: firstname.lastname@example.com
8	Backup managed by group	string		Name of the primary support group responsible for managing the backup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Column	Required column name	Type	Choice columns if applicable	Description and example
				Examples: App Engine Admins

2. After populating the Microsoft Excel spreadsheet, save it in a known location for easy access to upload.

Validate imported staging records

Validate the imported staging records from your import task to find missing, duplicate, and invalid data.

Before you begin

Role required: ot_excel_import_user

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the **List** () icon.
3. Under the OT Excel SGC - Import Task module, select one of the available lists.
4. Select the Import Task record that you want to validate.
5. Ensure you're the assigned to the import task so you can see the **Validate** UI action.

   Note: If you aren't in the **Assigned to** field of the import task, click the **Assign to me** UI action before proceeding with the next step.

6. Click the **Validate** UI action.
   Once the validation process is complete, the **State** field of the Import Task record changes to **Validation complete**. The **Validation state** of the staging records created can update to one of the following values.
   - Valid
   - Invalid
   - Partially invalid

   If invalid, the **Validation comments** field contains the cause or causes of the invalid state.

   If an imported staging record matches an existing configuration item (CI) in the CMDB, you can preview the existing OT records. For more information, see Preview existing OT records in the CMDB.

What to do next

For valid records, you can directly trigger the Configuration Management Database (CMDB) import. For more information, see Trigger a CMDB import for valid staging records.

To resolve invalid or partially invalid records, you can optionally create remediation tasks. For more information, see Create a remediation task for invalid staging records.

Managing Validations

Validation enables you to review and manage the imported data in the staging table.

Validations to be executed:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Missing correlation id (Correlation id)
- Missing parent correlation id in case the type is Control module (Control module parent id)
- Missing serial number (Serial number)
- Missing transformed name (Transformed name)
- Missing MAC Address (validation is executed on column MAC Address 1)
- Missing type (Type)
- Missing rack number (Rack number)
- Missing slot number (Slot number)
- Equipment model entity path does not exist (Equipment model entity path)
- Site name provided is invalid (Site name)
- Validate duplicates on transformed name (Transformed name)

  Note: This validation is skipped for control modules.

- Validate duplicates on MAC Address (check on all MAC Address 1 columns)
- Validate duplicates on Serial number column (Serial number)
- Validate duplicates on Correlation id column (Correlation id)
- Validate duplicates on rack and slot numbers

  Note: This validation is only for control modules.

- Validate Has Module and Control module Parent ID

  Note: This validation is only for PLCs and control modules.

- Validate Invalid types - Compare against the default Excel type to OT device type mapping through the *sn_otsm_sgc.SGOTAssetImportExtensionPoint* extension point implementation.

  If you have additional mappings, create an extension point implementation for the base system *sn_otsm_sgc.SGOTAssetImportExtensionPoint* extension point.

For more information about adding a custom implementation for device classification, see Add a custom implementation for device classification.

Preview existing OT records in the CMDB

Preview existing Operational Technology (OT) device records in the Configuration Management Database (CMDB) before you import any new records from the staging table. By previewing existing records, you can avoid reconciling or merging unrelated records.

Before you begin

Role required: ot_excel_import_user

About this task

If a matching configuration item (CI) is in the CMDB when you import OT devices from the staging table, existing records may reconcile or merge with new records. Matching CIs include the hostname, MAC address, or serial number. To avoid accidentally reconciling or merging records, you can preview the existing records that share the matching CIs with the records in the staging table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the **List** () icon.
3. Under the OT Excel SGC - Import Task module, select one of the available lists.
4. Select an Import Task record that you want to verify has any matching CIs.
5. In the Validation comments column, check if a matching CI has been found.
   The Validation comments column explains the matching CI that was found and contains a link to the matching CI. When a matching CI is found in the CMDB, the Validation state is set to **Partially Valid**. The following table lists the matching CI validation comments.

Matching CI validation comments

Matching CI	Validation comment
Hostname	Same transformed name found for another CI:<Link to CI>
MAC address	Same MAC address [MAC address] found for another CI:<Link to CI>
Serial number	Same serial number [serial number] found for another CI: <Link to CI>

6. **Optional:** View the matching CI by selecting it from the Matching CI in the CMDB column.

Trigger a CMDB import for valid staging records

Trigger a Configuration Management Database (CMDB) import for your valid staging records to directly import them into the CMDB

Before you begin

Role required: ot_excel_import_user

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the **List** () icon.
3. Under the OT Excel SGC - Import Task module, select one of the available lists.
4. Open the Import Task record that you want to trigger the CMDB import for.
5. Ensure you are assigned to the import task so you can see the **Trigger CMDB Import** UI action. If you are not in the **Assigned to** field of the import task, click the **Assign to me** UI action before proceeding with the next step.
6. Click the **Trigger CMDB Import** UI action.
7. Review the newly imported OT devices in OT List module in the Industrial Workspace.

Create a remediation task for invalid staging records

After running validations for the Operational Technology (OT) device data imported with the Service Graph Connector for Microsoft Excel, optionally create a remediation task to resolve invalid staging records.

Before you begin

Role required: ot_excel_import_user

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task
You can optionally create remediation tasks to resolve invalid staging records. For more information about the validation errors that can occur for your staging records, see Managing Validations.

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. Select the **List** () icon.
3. Under the OT Excel SGC - Import Task module, select one of the available lists.
4. Select the Import Task record that you want to create remediation tasks for.
5. Ensure that you are assigned to the import task so that you can see the **Create Remediation Tasks** UI action.
   If you are not in the **Assigned to** field of the import task, click the **Assign to me** UI action before proceeding with the next step.
6. Click the **Create Remediation Tasks** UI action.

Result
Remediation tasks are created for the invalid staging records. To access the remediation tasks in the Import Task record, select the **Remediation Tasks** list.

Note: One remediation task is created for all invalid staging records that belong to the same site.

When you view the remediation task record, you can also view the staging records associated with it by selecting the **Staging Records** tab.

Create an Operational Technology device in the Industrial Workspace

Create an Operational Technology (OT) device in the Industrial Workspace.

Before you begin
Role required: cmdb_ot_editor

About this task
You can manually create an OT device in the Industrial Workspace, which creates an OT Entity [cmdb_ot_entity] record and associates it with a CI.

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. Select the **List** () icon.
3. Under the **Operational Technology (OT)** module, select one of the following lists.
   - All OT Devices
   - OT Supervisory Systems
   - OT Control Systems
   - OT Field Devices
   - OT Computer and Servers
   - OT Network Gear
   - Industrial IoT (IIoT)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- OT Systems
- Unclassed OT Devices

4. Select **Create New CI**.
5. In the Create OT CI tab, complete the following sections as needed.
   - Select class
   - Required attributes
   - Additional attributes
   - Relationship definition
   - Review
6. Select **Create**.
7. In the New CI created window, select **Review new CI** to redirect you to the form of the created OT CI.
   If there's an existing CI, select **Review existing CI**.
8. On the form, fill in the following fields.

CI form

Field	Description
Display name	The name of the OT device displayed in the record. **Note:** You can add any string value to this field. Multiple devices can have the same OT display name. This is meant for easier understanding of the OT device and is different from the unique CI name generated when you import OT devices from the staging table.
Purdue level	Assigned Purdue level. The level ranges are 0–5. **Note:** To learn more about the Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.
Device criticality	Measure of the relative risk to the site process if the device fails: - 1 - Most critical - 4 - Not critical
Site	The top-level parent entity, or industrial site, where the device is located or assigned to.

9. Select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Edit or view OT devices after import or discovery

Use the options on the Operational Technology (OT) menu to edit or view detailed information for the OT devices in your enterprise.

Before you begin

Import your Operational Technology device data in any of the following ways:

- Run IT Discovery for OT Networks. For more information, see IT Discovery for Operational Technology (OT) Networks.
- Use an Operational Technology Certified Service Graph Connector from the ServiceNow Store.

Role required: cmdb_ot_viewer, cmdb_ot_editor, cmdb_ot_admin, or admin

About this task

If you have an assigned cmdb_ot_viewer role, you can only view OT devices. If you have an assigned cmdb_ot_editor or cmdb_ot_admin role, you can edit OT device records in the following ways:

- Edit OT device records individually on the ServiceNow AI Platform.
- Bulk edit multiple OT device records from the Industrial Workspace list view.

Procedure

1. To edit one OT device record ServiceNow AI Platform, follow these steps.
   a. Navigate to **All** > **Operational Technology (OT)** and select one of the following menu items:

      All OT Devices

      By default, this list does not include control modules.

      All OT Devices by IP Address

      When you view the All OT Devices by IP Address list, note the following:

      - An OT device with multiple IP addresses is displayed once per assigned IP address.
      - Select the name of the OT device to open the OT device record. Selecting the IP address that is displayed for the record opens the record of only the IP address.
      - You **cannot** create a new OT device record from this list.

      OT Control Systems

      By default, this list does not include control modules.

      OT Control Systems with Modules

      When you view the OT Control Systems with Modules list, note the following:

      - The list view displays all the Control Modules grouped by their parent Control System.
      - You cannot create a new OT device record from this list.

   b. In the **OT device** column, select the OT device that you want to edit.

   c. On the form, fill in the fields.

   d. Click **Update**.

2. To bulk edit multiple OT device records Industrial Workspace, follow these steps.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **All** > **Industrial Workspace**.

b. Open the list ( ) view and select one of the following lists available under **Operational Technology (OT)**.
   - OT Supervisory Systems
   - OT Control Systems
   - OT Field Devices
   - OT Computer and Servers
   - OT Network Gear
   - Industrial IoT (IIoT)
   - Unclassed OT Devices

c. Select the check box next to each OT device that you want to edit.

> **Note:** You can only bulk edit OT devices with the same **Class** field. You can't use the bulk edit feature for OT devices with different classes.

d. To edit the configuration item (CI) fields, select the **Edit** button and edit the form fields as needed.

> **Note:** The maximum number of records that you can bulk edit the CI fields for is the records shown on a single page.

e. Click **Update**.

f. To edit the OT device details, select the **Edit OT details** button and edit the form fields as needed.

> **Note:** Bulk editing OT details is a background job that can take time to complete. If the background job is busy, you can't bulk edit other OT device records.

OT device related items and related lists

The All OT Devices, All OT Devices by IP Address, and All OT Devices by CI menu options contain several related items and lists.

Related items

This section lists any related or subordinate items that are associated with this OT device.

> **Note:** Not all OT devices display the following related lists. For OT devices in an Operational Technology class or extended class, the following related lists are displayed. For OT devices categorized in a different hardware class, such as Windows Server, an instance admin must add the related lists to the form.

1. To view the related records, click the name of the related item (for example, Memory Modules).
2. To add a configuration item (CI) relationship for this OT device, click the add CI relationships icon ( ). Use the search field to find the CI item that you want to create a relationship for.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. To access the Dependency View form to see a pictorial depiction of the OT device relationships, click the show dependency views icon ().
4. To change the settings that govern how the related items appear and are filtered, click the settings icon ().

OT device related lists

Related list	Description
IP Address	The IP addresses, IP versions, net masks, network partition identifiers, NIC numbers, and configuration items that are associated with the OT device.
Network Adapters	The names, MAC addresses, IP addresses, Netmasks, MAC manufacturers, and Dynamic Host Configuration Protocol (DHCP)-enabled indicators. It includes statuses of the network adapters that are associated with the OT device.
Serial Numbers	The serial numbers, validity indicators, and serial number types that are associated with the OT device.
Equipment Model Entities	The equipment model entities that are automated by the OT device.
OT Subnet Mappings	The subnet mapping that associates an OT device with an equipment model entity.
OT Control Modules	The control modules that are associated with the OT device of type OT control system or extended classes (for example, PLC). Each OT control module that has an "Owned by: Owns" relationship with the OT Control System record that is displayed. In the platform, the user can create an OT Control module. You can choose from the following Input/Output values depending on the **Module type** field: • None • Local • Remote • Distributed
CMDB 360	The related CMDB 360 data in the CMDB 360 [cmdb_multisource_data] table.
Memory Modules	The serial numbers, validity indicators, and serial number types for the memory modules that are associated with the OT device.
Software Installed	The application software, if any, that is installed for the OT device.
OT Vulnerable Items	The vulnerable items that are associated with the OT device.
OT Incidents	The OT incidents that are associated with the OT device.
OT Change Requests	The OT Change requests that are associated with the OT device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT device related lists (continued)

Related list	Description
External System Metadata	The URL of the device in the source system, discovery source, and updated devices that are associated with the CI. The URL is automatically populated by the source system through the service graph connector.
OT Protocols	This is applicable for protocol converter class. The protocols, description, vendor, and version that are associated with the protocol converter class.
Backup Information	The Backup Information object associated with the current CI.
Device to Device Connections	Shows the network connections an OT device has with other devices.
IP Network Subnets	Shows all subnets the device is associated with.
Key Value	Additional information related to the OT device that's populated with the available OT integrations and captured as Key value pairs.
Software Instance	Captures the software installed on the OT device if Software Asset Management isn't available. **Note:** If Software Asset Management is installed and entitled, the software installed data is available in the Software Installation related list.
Firmware Installation	Firmware associated with the OT device.
VLAN Configurations	Captures the following VLAN information associated with the OT device. • VLAN ID • VLAN Tag • Subnet • VLAN Type

Operational Technology device form

Use the Operational Technology (OT) device form to edit the detailed information for the OT devices in your enterprise.

Operational Technology device form

Field	Description
OT display name	The name of the OT device displayed in the record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology device form (continued)

Field	Description
	Note: You can add any string value to this field. Multiple devices can have the same OT display name. This is meant for easier understanding of the OT device and is different from the unique CI name generated when you import OT devices from the staging table.
OT device type	The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example: An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is **server** and its device type is **HMI**. **Note:** In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select **No OT Function**. For OT devices where the device type is unknown, select **Unknown**.
Device criticality	The measure of the relative risk to the site process of failure of the device. For example: • 1 - Most critical • 4 - Not critical
Site	The top-level parent entity, or industrial site, where the device is located or assigned to.
Purdue level	The assigned Purdue level. Ranges 0–5. **Note:** To learn more about Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.
Zone	The area within the site location that the device is assigned to.
Class	The name of the assigned class for the OT device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology device form (continued)

Field	Description
	Note: For a listing and explanation of CI classes, see Operation Technology (OT) extension classes.
Status	Status of the OT device: **--None--** No assigned status. **Absent** OT device is absent in your facilities. **In Maintenance** OT device is in maintenance and currently is off line. **In stock** OT device is in stock in your facilities. **Installed** OT device is installed in your facilities. **Pending Install** OT device is pending installation in your facilities. **Pending repair** OT device is pending repair but is not online yet. **Retired** OT device is retired. **Stolen** OT device has been stolen.
Discovery source	The Discovery source for the OT device data. For example, SG-OT Excel Import, if you imported the OT device from a Microsoft Excel spreadsheet using the Integration Hub ETL. To learn more, see Service Graph Connector for Microsoft Excel.
Infrastructure Relationships	Shows the relationship of OT device with other the OT devices and the equipment model entities.
Service Relationships	Shows the relationship of OT device with the equipment model entities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology device form (continued)

Field	Description
CI Timeline	Shows the timeline of OT incidents, OT change, and audit history associated with the OT device.
The following fields only apply to the Programmable Logic Controller (PLC) Class Records:	
Key switch	The Key switch modes: **Remote mode** You can change the configuration of the PLC. **Local mode** By default mode, you can't change the configuration of the PLC.
Switch position	The Switch position of the PLC has the following positions: • **Run** • **Program** • **Remote** • **Stop** • **Test** By default, the switch position is set to **None**. When the switch position is set to **Remote**, the Switch remote modes are enabled.
Switch remote mode	The Switch remote of the PLC has the following modes: • **Run** • **Program** • **Test** • **None**
Asset	When configuration items (CIs) are created in the Configuration Management Database (CMDB), asset records are created. The asset record contains the model category of the CI. For more information about the model categories for Operational Technology (OT), see Model categories for Operational Technology. To view the model category for an OT device, complete the following:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology device form (continued)

Field	Description
	1. Navigate to **All** > **Operational Technology (OT)** > **All OT Devices**. 2. Select the OT device that you want to view the asset record for. 3. Next to the **Asset** field, select the **Preview this record** ( ) icon. 4. Select **Open Record**.
The following fields only apply to the following class records. • OT Supervisory System • OT Control System • OT Field Device • Unclassed OT Device	
Is Virtual	If selected, indicates that the OT device is virtual.

Convert an IT hardware device to an OT device

If you've identified IT hardware devices that belong to the OT network, you can convert these IT Configuration Items (CI) into OT devices.

Before you begin

Role required: cmdb_ot_admin or admin

About this task

This task is applicable to all IT hardware devices.

Procedure

1. Select an IT CI.
   For example, you can navigate to **All** > **Configuration** > **Base Items** > **Computers**.
2. Select the IT hardware device that you want to convert to an OT device.
3. In the Related Links module, select **Add OT Device Details**.

   The OT Device form is displayed.
4. Fill in the fields on the OT Device details form.
5. Select **Update**.
6. To view the converted OT Device, navigate to **All** > **Operational Technology (OT)** > **All OT Devices**.

Result

The selected IT hardware device has been converted to an OT device.

Alternatively, you can select multiple IT hardware devices and convert them into OT devices in a bulk edit. For more information, see Convert IT hardware to OT devices in a bulk edit.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Convert IT hardware to OT devices in a bulk edit

Choose multiple IT hardware devices and convert them to OT devices in a bulk edit so that you can edit your records more quickly and efficiently.

Before you begin

Role required: cmdb_ot_admin or admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Workspace**.
2. In the Industrial Workspace, navigate to the All IT Hardware list.
3. **Optional:** If you want to filter the All IT Hardware list, do the following actions:
   - Select the filter Filter icon.
   - Add the filter that you want applied to the list.
   - Select **Update**.
4. Select the check box next to each of the IT hardware devices that you want to convert.
   If you want to select all IT hardware devices in the list, select the check box next to the Name column.
5. Select the **Convert to OT devices** button.
6. On the form, fill in the fields.

Convert to OT devices form

Field	Description
OT Device Type	The category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example: An IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Therefore, its class is **server** and its device type is **HMI**. **Note:** In some cases, there are OT devices with no OT function or OT devices where the device type is unknown. For OT devices with no OT function, select **No OT Function**. For OT devices where the device type is unknown, select **Unknown**.
Device Criticality	Measure of the relative risk to the site process if the device fails: - 1 - Most critical - 4 - Not critical
Purdue Level	Assigned Purdue level. The level ranges are 0–5.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: To learn more about the Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.
Zone	area within the site location that the device is assigned to.
Site	Top-level parent entity, or industrial site, where the device is located or assigned to.

7. Select **Convert**.
   A banner appears to notify that the process has started. To check the All OT Devices list for updates, you can select the link in the banner.

Result
The selected IT hardware devices have been converted into OT devices.

You can also use the Bulk Update Ruleset for Reassigning IT to OT feature to create a scheduled job that automatically converts IT hardware to OT devices. For more information, see Automatically convert your IT records to OT devices.

Convert your OT devices to IT hardware devices in a bulk edit

Bulk edit your Operational Technology (OT) devices to remove the OT device details. Then convert your OT devices to IT hardware devices.

Before you begin
Role required: cmdb_ot_admin or admin

About this task
If you encounter OT devices that don't have an OT function and should be classified as IT hardware devices, you can select and edit multiple OT devices in a bulk edit to convert them to IT hardware devices.

Procedure
1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Workspace.**
2. In the list view, select one of the following lists.
   - OT Computer and Servers
   - OT Network Gear
   - Industrial IoT (IIoT)
3. Select the OT devices that you want to convert to IT hardware devices.
   If you want to select all OT devices in the list, select the check box next to the OT device column.
4. Select the **Remove OT device details** button.
   A dialog box appears that asks you to confirm that you want to remove the OT device details but keep all the other configuration item details.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: None of the CI details, network adapters, or IP addresses are removed. Only the OT-specific data is removed.

5. Select **Confirm**.

Result

The OT device details are removed from the selected OT devices and the OT devices are converted to IT hardware devices. You can view these IT hardware devices in the IT Hardware list view on the Industrial Workspace.

Map IP addresses to OT devices

You can use the `SyncIPAddressToOT` scheduled job to update and synchronize the IP address information for all the available OT devices. The `SyncIPAddressToOT` scheduled job acquires the IP address information from the IP address (cmdb_ci_ip_address) table and adds it to the IP address field of the CI.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
2. In the **Scheduled Jobs** page, type `SyncIPAddressToOT` in the **Search** filter and hit enter to find the scheduled job.
3. Select `SyncIPAddressToOT`.
4. In the Scheduled Script ExecutionSyncIPAddressToOT page, select **Execute Now**.

View and edit device to device connections

View and edit device-to-device connections for your Operational Technology (OT) devices using the Device to Device Connections list in the Industrial Workspace.

Before you begin

- Ensure you have the Industrial Core [sn_ot_core] plugin installed.
- Role required:

Role	Description
cmdb_ot_viewer	Required to read or view device to device connections.
cmdb_ot_editor, cmdb_ot_isa_editor	Required to edit, create, or delete device to device connections.

About this task

The Device to Device Connections uses the `OTNetworkUtils` script include for the OT device look-up logic. The look-up logic identifies the corresponding Source and Destination CIs based on IP addresses, sites, and managed networks.

The Device to Device Connections list shows fields from both the OT Device Network Connection [sn_ot_device_network_connection] table and the CI relationships [cmdb_rel_ci] table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the **List** () icon.
3. Under the **OT Network** module, select the **Device to Device Connections** list.
4. If needed, edit the following fields by selecting the checkbox next to an device to device connection and clicking **Edit**.

Device to Device Connections form

Field	Description
Parent	Configuration item (CI) record of the source device.
Child	CI record of the destination device.
Source IP Address	IP address assigned to the source device.
Source Device CI	CI record of the source device.
Source MAC Address	MAC address of the source device.
Destination IP Address	IP address assigned to the destination device.
Destination Device CI	CI record of the destination device.
Destination MAC Address	MAC address of the destination device.
Destination Port	Network port used by the destination device for communication.
Last Communication Time stamp	Date and time when the devices last communicated. **Note:** Any device-to-device connection record with a Last Communication Time stamp of 90 days or longer is deleted. To edit the Last Communication Time stamp, perform the following actions. **a.** Navigate to **All** > **Instance Scan** > **Table Cleanup**. **b.** In the sn_ot_device_network_connection record, edit the **Age in seconds** field as needed. The default is `7,776,000`.
Transport Protocol	Protocol used for data transfer. For example, TCP, UDP.
Application Protocol	Application-level protocol used. For example, HTTP, Modbus, FTP.
Source Managed Network	Managed network segment where the source device resides.
Destination Managed Network	Managed network segment where the destination device resides.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Discovery Source	Source that's providing the connection information.

5. Select **Save**.

Result

To view a device-to-device connection for an OT device, you can access the Device to Device Connections related list in the OT device record. For more information about related items and related lists for OT devices, see Edit or view OT devices after import or discovery.

Managing Network Intrusion Detection System appliances

If you have the cmdb_nids_admin or admin role, you can assign metadata attributes to Network Intrusion Detection System (NIDS) class records from the NIDS menu in the ServiceNow AI Platform.

A Network Intrusion Detection System helps manage the import of IT and OT devices from supported integrations. Assigning meta data such as location and NIDS network type to NIDS records helps you distinguish between detected OT and IT devices, and automatically adds the related meta data to the created records. Users with the cmdb_nids_admin or admin role can edit the **NIDS Assigned Meta Data** tab and view the changes made by the user in the Activity Stream.

Note: Manual creation for an NIDS record in the table is restricted from the list view or the form view of the records.

For more information about the NIDS class records, see Network Intrusion Detection System (NIDS) CI extension class.

If a NIDS record has the Validated field set to true, then when any of the following attributes of the NIDS are changed on the NIDS form, a warning message is displayed.

- NIDS network type
- NIDS source name
- NIDS source ID

If the NIDS record with any detects::detected by relationships is deleted, a warning message is displayed.

You can use the Network Intrusion Detection Systems (NIDS) Guided Setup to lead you through:

- Configuring users and roles for users that do not already have an account in an instance
- Importing NIDS records from Operational Technology (OT) Certified Service Graph Connectors to designate if NIDS appliances are running on OT or IT networks
- Validating NIDS so that detected devices can be imported. For more information about validating NIDS, see Validate the NIDS.

To access the NIDS Guided Setup, navigate to **Network Intrusion Detection Systems (NIDS)** > **NIDS Guided Setup**.

To assign an appliance as a manager for NIDS sensors that detect devices, navigate to **Network Intrusion Detection Systems (NIDS)** > **Managers** to edit applicable "management consoles" or "central managers" records.

- Review the Sensors list to ensure that there is not currently a device assigned as manager.
- For any devices that do not function as sensors, change **is manager** to **True**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For information about the `NIDSUtils` script include that copies NIDS-assigned meta data to detected devices, see Script includes installed with Operational Technology Manager.

Related topics

Network Intrusion Detection System (NIDS) CI extension class

Script includes installed with Operational Technology Manager

Validate the NIDS

Validate the NIDS to import the devices from the ETL that were detected by the sensor. The sensors can only pass the validation if they aren't in learning mode as such sensors aren't eligible for device import.

Before you begin

It's recommended that you have the Common Service Data Model plugin installed. The Service Graph Connector aligns with the life cycle data models as per the Configuration Management Database (CMDB) standards. For more information, see Implementing the CSDM framework in stages.

Role required: cmdb_nids_admin

About this task

The **Life Cycle Stage** and **Life Cycle Stage Status** fields are used to capture the learning mode of a sensor. If the Life Cycle Stage field is set to **Operational** and Life Cycle Stage Status is set to **Learning Mode**, then validation is unsuccessful. If the Life Cycle Stage Status field is set to **In Use**, the validation is successful.

Procedure

1. Navigate to **All** > **Network IDS Appliance (NIDS)** > **Sensors**.
2. If there are any management consoles or central managers in the list, do the following actions:
   a. Click **edit the record**.
   b. In the **NIDS Admin Configuration** tab, select **Is NIDS manager** to set the **Validated** column true.
3. In the NIDS Admin Configuration section, make sure that the **Life Cycle Stage Status** value is not Learning Mode.
   Otherwise, the validation fails.
4. Select the **NIDS network type**.

   The Network type must be selected based on the location of the sensor.

   Note: The network type OT creates the OT device record. The network type IT does not create the OT device records.

5. In the **NIDS Assigned Meta Data** tab, check that all the devices discovered by the NIDS are entered.
6. Click **Validate**.

   Note:

   The zone value is populated by the ETL. If a zone value is manually entered on the NIDS record, it is overridden what is populated by the ETL.

   If the NIDS record is not validated, the devices are not imported from the ETL that were detected by the sensor.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
Alternatively, you can validate more than one NIDS sensor through a bulk validation. For more information, see Validate multiple NIDS sensors at once.

Validate multiple NIDS sensors at once

Validate multiple NIDS sensors at once through a bulk validation so that you can edit your records more quickly and efficiently.

Before you begin
Role required: cmdb_nids_admin

About this task
You can use bulk validation to validate multiple NIDS sensors at once instead of individually validating each NIDS sensor.

Note: Carefully review the NIDS sensors by discovery source and proceed with caution while bulk validating.

Procedure
1. Navigate to **All** > **Network IDS Appliance (NIDS)** > **Sensors**.
2. Select the check boxes the sensor records that you want to validate.
3. Select the **Validate Sensors** button.

Result
If the sensors you validated have a **Life Cycle Stage Status** of In Use, a successful validation message appears.

If the selected sensors have a **Life Cycle Stage Status** of Learning Mode or the **Validated** column is set to true, an error message appears alerting you that one or more sensors in learning mode haven't been validated or already validated. You should consider changing the **Life Cycle Stage Status** column to In Use to proceed with the bulk validation.

Modeling an Operational Technology system service

You can model an Operational Technology (OT) system service to create other control systems, such as a distributed control system (DCS).

An OT system service refers to a category of technology and systems that are used to manage, control, and monitor physical processes, machinery, and industrial operations. OT system services are typically employed in sectors such as manufacturing, energy, utilities, and transportation.

OT system services can include the following.

- Distributed Control Systems (DCS)
- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)
- Safety Instrumentation Systems (SIS)
- Manufacturing Execution Systems (MES)
- Process Control Systems
- Transportation Management Systems
- Energy Management Systems
- Building Management system services (BMS)

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These system services collectively ensure that industrial processes run efficiently and safely.
DCS example

You can model OT system services to create other control systems. For example, you can model a distributed control system (DCS) and all related components (PLCs, control modules, EWS, RTU, HMI, SCADA, and so on). A DCS is a platform for automated control and operation of a plant or industrial process. It coordinates and supervises the entire plant of many varying processes.

A DCS is a process-oriented system that uses closed loop control. The following table describes the components of a DCS.

DCS Components

Component	Description
Operator stations	Heart of DCS, operators view process, monitor alarms, and alerts.
Servers, EWS, Historians	Data collection and data exchange for hardware configurations.
Controllers, I/O modules	Data exchange to servers.
Field devices	Devices such as transmitters, switches, actuators, and valves.

A DCS differs from the centralized control system wherein a single controller at central location handles the control function but in a DCS, each process element, machine, or group of machines is controlled by a dedicated controller.

Create an Operational Technology system service

Create an Operational Technology (OT) system service to model a distributed control system (DCS) and all of its related components, such as control modules and programming logic controls (PLCs).

About this task

You can create an OT system service in the following locations:

- ServiceNow AI Platform in the **OT Systems** list
- Industrial Industrial Workspace list view

Before you begin

Role required: admin

Procedure

1. If you want to create an OT system service on the ServiceNow AI Platform, complete these actions:
   a. Navigate to **All** > **Operational Technology (OT)** > **OT Systems**.
   b. Select **New**.
   c. On the form, fill in the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT System Service Form

Field	Description
Display name	Used to populate the display name of the OT system service.
Name	Host name of the OT system service.
ISA entity site	ISA entity site that the OT system service belongs to.
Manufacturer	Name of the manufacturer of the OT system service.
Model number	Manufacturer's model number for the OT system service.
Short description	Brief description of the OT system service.
Details	
Owned by	Name of the primary owner of the OT system service.
Managed by	Name of the primary manager of the OT system service.
Business criticality	Measure of how critical, or important, the system service is. Examples: ▪ High or Most critical ▪ Medium or somewhat critical ▪ Low or Less critical ▪ None or not critical
Support Group	Name of the primary support group for the OT system service.
Managed By Group	Name of the group that manages the OT system service.
Operational status	Status of the system service.

d. Select **Submit**.

2. If you want to create an OT system service in the Industrial Workspace list view, complete these actions:

a. Navigate to **All** > **Industrial Workspace**.

b. Select the List () icon.

c. Under the **Operational Technology (OT)** module, select the **OT Systems** list.

d. Select **New**.

e. On the form, fill in the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT System Service Form

Field	Description
Display name	Used to populate the display name of the OT system service.
Name	Host name of the OT system service.
ISA entity site	ISA entity site that the OT system service belongs to.
Manufacturer	Name of the manufacturer of the OT system service.
Model number	Manufacturer's model number for the OT system service.
Short description	Brief description of the OT system service.
Details	
Owned by	Name of the primary owner of the OT system service.
Managed by	Name of the primary manager of the OT system service.
Business criticality	Measure of how critical, or important, the system service is. Examples: ▪ High or Most critical ▪ Medium or somewhat critical ▪ Low or Less critical ▪ None or not critical
Support Group	Name of the primary support group for the OT system service.
Managed By Group	Name of the group that manages the OT system service.
Operational status	Status of the system service.

f. Select **Save**.

What to do next

Now you can add OT devices to the system service. For more information, see Add a device to an Operational Technology system service.

Add a device to an Operational Technology system service

Add an Operational Technology (OT) device to an OT system service to create a relationship between the equipment model entity that the device belongs to and the OT system service.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the List () icon.
3. Under the **Operational Technology (OT)** module, select the **OT Systems** list.
4. Select the OT system service you want to add a device to.
5. In the **Related Records** tab, select the **Associated OT Devices** related record.
6. Select **Add**.
7. Select the check box next to one or more OT devices.
8. After you choose all the OT devices, select **Add**.

Result

After you add the OT devices, the following relationships are created:

- The Depends on::Used by relationship between the selected configuration item (CI) and the OT system service
- The Managed by::Manages relationship between the OT system service and CI's equipment model entity.

Map an Operational Technology system service to an equipment model entity

Map an Operational Technology (OT) system service to an ISA equipment model entity by enabling a scheduled job. When the relationship between an OT device and an equipment model entity changes, the scheduled job recomputes the relationship between the OT system service and the equipment model entity.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
2. Select the Show/hide filter () icon.
3. Add the following filter.
   `[Name] [is] [Map OT Systems to ISA Entities]`
4. Select the **Map OT Systems to ISA Entities** scheduled job record.
5. Next to the **Active** field, select the check box.
6. In the **Run** field, select the option that best fits your needs.
7. Select **Update**.

View the dependency map for an Operational Technology system service

View the dependency map for an Operational Technology (OT) system service to see the graphical representation of the hierarchical structure of the selected OT system service and its relationship with other entities in the production process.

About this task

You can view the dependency map for an OT system service in the following locations:

- ServiceNow AI Platform in an OT system service record
- Industrial Workspace in an OT system service record

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: cmdb_ot_editor

Procedure
1. If you want to view the dependency map for an OT system service on the ServiceNow AI Platform, complete the following actions:
   a. Navigate to **All** > **Operational Technology (OT)** > **OT Systems**.
   b. Select the OT system service record you want to view the OT dependency map for.
   c. Select **View OT Dependency map**.
2. If you want to view the dependency map for an OT system service in the Industrial Workspace, complete the following actions:
   a. Navigate to **All** > **Industrial Workspace**.
   b. Select the List ( ) icon.
   c. Under the **Operational Technology (OT)** module, select the **OT Systems** list.
   d. Select the OT system service record you want to view the OT dependency map for.
   e. Select **View OT Dependency map**.

Automatically convert your IT records to OT devices

Create a scheduled job that automatically converts your IT hardware to Operational Technology (OT) devices by using the Bulk Update Ruleset for Reassigning IT to OT feature. This scheduled job adds OT entity details to all the IT hardware that you want to convert at once.

Before you begin
Role required: admin or cmdb_ot_admin

About this task
You may have configuration items (CIs) classed as IT hardware that you want to create OT entity records for. Follow these general guidelines:

- Make sure that the fields you use apply to the filter criteria conditions in steps 3 to 4. Verify that the data set doesn't exceed 1 million records so that you can avoid performance-related issues.
- Create separate scheduled job definitions for the separate CI classes in steps 3 to 6. This way, you can filter each CI level and define the OT entity default values.
- Use the Class field in the filter to query only specific CI classes in step 3.

  Note: Only the hardware class and its extended classes are used in the source table.

- Use the **Preview** button to verify the records selected for further review in step 4.
- Verify the data in the **OT Entity Default Configuration** tab in step 5. The OT entity records are created using these default values.

You can also manually convert the IT hardware to the OT devices. For more information, see Convert IT hardware to OT devices in a bulk edit.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **OT Manager Admin** > **Automated IT OT Bulk Contextualization**.
2. Select **New**.
3. On the **Filter Criteria - OT Devices** tab, set the source table and filter criteria to identify the CIs that you need to convert.

   For example, if you want to add the OT entity details for all computers that are imported into the system that have a prefix of COMP, select the source table as **cmdb_ci_computer** and then add the filter criteria as **[Name] [starts with] [COMP]**, **[Class] [is] [Computer]**, and **[OT device details] [is empty]**.

   You can also use CMDB groups to group IT CIs based on additional information, such as Software Installed, so that you can convert them to OT devices. For more information, see Use CMDB groups to add OT context to IT CIs.

   Note: If you're using a CMDB group, the **Filter Criteria - OT Devices** tab shown in this step isn't visible.

4. Verify the number of records that were chosen from the filter condition you set by selecting the **Preview** button.
   The OT entity details are added for these records, such as OT Device Type and Device Criticality.
5. On the **OT Entity Default Configuration** tab, fill in the fields.
   The fields in the following table provide the default values that are added to the OT entity records or the OT-related metadata.

OT Entity Default Configuration form

Field	Description
OT Device Type	Category type that the OT device is classified as. The device type is also the function that the device plays on the OT network. For example, an IT device, such as a server, can be converted to an OT device, and the function it plays on the network is an HMI. Its class is server and its device type is HMI. **Note:** In some cases, OT devices have no OT function or the device type is unknown. Where the OT devices have no OT function, select **No OT Function**. Where the OT devices have an unknown device type, select **Unknown**.
Device Criticality	Measure of the relative risk to the site process if the device fails: ○ 1 - Most critical ○ 4 - Not critical

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Purdue Level	Assigned Purdue level. The level ranges are 0–5. **Note:** To learn more about the Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.
Zone	Area within the site location that the device is assigned to.
Site	Top-level parent entity, or industrial site, where the device is located or assigned to.

6. In the **Run** field, select a scheduled time for this job to run.
7. Select the check box next to the **Active** field.
8. Select **Submit**.
9. To run the job immediately, select **Execute Now** in the record.
   When you select **Execute Now**, a confirmation modal is shown to ensure you want to create OT entity records from the table specified in the **Filter Criteria - OT Devices** tab. For example if you're creating a scheduled job for the source table cmdb_ci_computer, you will see the following message:

   This action will trigger the scheduled job which creates OT entity records for 3 records from "cmdb_ci_computer" table as per the query condition. Are you sure to want to proceed?
10. Select **Proceed**.

Use CMDB groups to add OT context to IT CIs

Use Configuration Management Database (CMDB) groups to group IT configuration items (CIs) based on additional information, like installed software. Then you can add Operational Technology (OT) context to the IT CIs.

Before you begin

Role required: admin or cmdb_ot_admin

About this task

Using CMDB groups doesn't change the class of the IT CI. It instead adds OT entity records to the IT CI, which captures the OT context.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

Follow these general guidelines:

1. Ensure the filter conditions on the CMDB Group returns unique set of CI records every time. For example, adding a filter condition such as **[OT device details] [is EMPTY]** ensures that only records without OT device details are considered.
2. Make sure the indexed fields are used as part of the filter criteria conditions. Ensure that the data set does not exceed 10,000 records to avoid performance related issues.

   Note: The CMDB Group API doesn't support retrieving records exceeding 10,000 or the limit defined by the following properties.

   - glide.cmdb.query.max_results_limit
   - glide.cmdb.group.max_ci_limit

   To address this, these properties need to be adjusted to allow for larger query results if the CMDB query contains more records than the current limits permit.
3. Make sure to create an Automated IT to OT Bulk Contextualization (sn_automated_it_ot_bulk_contextualization) record per CMDB Group to have filtering at a group level and define respective OT entity default values.
4. Validate the data in the **OT Entity Default Configuration** tab. OT entity records are created using these default values.

Procedure

1. Define a CMDB group with the required filter criteria that identifies the right IT CIs. For more information, see CMDB groups.
2. Create an Automated IT to OT Bulk Contextualization (sn_automated_it_ot_bulk_contextualization) record associated with the CMDB group. Creating this record adds OT context to IT CIs through the OT entity details.

   For more information about how to create an Automated IT to OT Bulk Contextualization record, see Automatically convert your IT records to OT devices.

   Note: The **Filter Criteria - OT Devices** tab isn't visible when using CMDB groups.
3. To create a record in **sn_automated_it_ot_bulk_contextualization_m2m_cmdb_group**, complete the following actions.
   a. Navigate to **All** > **Industrial Workspace Admin** > **OT Manager Admin** > **Automated IT OT Bulk Contextualization - Using CMDB groups**.
   b. Select **New**.
   c. In the **Automated IT to OT Bulk Contextualization** field, select the record created in step 2.
   d. In the **CMDB Group** field, select the CMDB created in step 1.
   e. Select **Submit**.

   You cannot create an Automated IT OT Bulk Contextualization record with more than 1 CMDB group. If you try to create a record with more than 1 group, the following error message is shown:

   An IT to OT contextualization record can't be associated with more than one CMDB group. If an IT to OT contextualization record associated with the CMDB group already exists, you can't create another record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The record associates the CMDB group with the Automated IT to OT Bulk Contextualization record.

For example, if you want to add OT entity details for all computers that have a specific HISTORIAN software installed, you need to create a CMDB Group that matches this filter critieria. Then create a scheduled job and link it to the CMDB Group for computers that have HISTORIAN software installed.

4. To run the job immediately, select **Execute Now** in the record.
When you select **Execute Now**, a confirmation modal is shown. The scheduled job can only process 10,000 CIs at one time. The message shown in the modal depends on the number of CIs you have. The following table shows examples of the messages you may see.

Confirmation modal example messages

Number of CIs	Message
Less than 10,000 CIs	This action will trigger the scheduled job which creates OT entity records for 2 records from the CMDB group "Name starts with H". Are you sure you want to proceed?
More than 10,000 CIs	Associated CMDB group has over 10K CIs. This action will trigger the scheduled job which creates OT entity records for the first 10K records and the remaining CIs will be processed in the next job run. Are you sure you want to proceed?

5. Select **Proceed**.

Create CMDB Data Certification Policy for Operational Technology

Create a CMDB Data Certification Policy for Operational Technology (OT) to validate and maintain accurate configuration item (CI) data.

Before you begin

Role required: sn_cmdb_admin

About this task

CMDB Data Certification policies help maintain the accuracy and reliability of data in the CMDB. The policies define when and how configuration items (CIs) are validated and automatically generate certification tasks for assigned reviewers.
You can use certification policies to:

- Periodically validate key attributes of CIs.
- Assign certification tasks to individuals or groups.
- Track and manage certification progress from a central workspace.

For example, you can create a policy that certifies IP Address, MAC Address, and Serial Number for all Control Systems located in Site A of a manufacturing plant.

Procedure

1. Navigate to **Workspaces** > > **CMDB Workspace** > **Management**.
2. From the Management page, navigate to **Management tools** > **Data Manager** > **Policies**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select **Create a new policy** and enter the following information for each parameter:

Parameter	Description
General Information	Enter the policy name and description, ensure the Policy type is set to Certification, and Select **Continue**.
Data Filter	Define the criteria for the policy, select **Apply filter** to preview the included CIs, and select **Continue**. Verify the records and select **Continue**.
Assignment	Select the Assignment type for the tasks that are created based on the policy and select **Continue**. You can choose to: ○ Assign the tasks to a user or a user group mentioned on the CI record. ○ Set static values as well. For example, we are assigning the tasks to the user group responsible for managing the Control Systems in the Site 1.
Options	In the Options section: ○ **Display fields** are visible to users in the list view when they click on review the CIs. Choose field values as per your requirement. ○ The **Certification fields** are the fields that are certified by the user. ○ Select the **Allow field updates** checkbox in case you want to allow users to fill in the field value. ○ In the **Days to complete** field, set the number of days to complete the created certification task. ○ In the **Instructions** field, you can provide additional information or instructions for users. Select **Continue**.
Schedule	In the **Schedule** page, enter values according to your requirement to configure the frequency of the policy to be triggered.
Review	Review the policy in detail and select **Publish Policy**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
You can view the policy in the **Published Policies** section on the main page after publishing.

Operational Technology Manager reference

Reference topics provide additional information about the Operational Technology Manager application.

Components installed with Operational Technology Manager

Several types of components may be installed with activation of the Operational Technology Manager application, including user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Plugins installed

Plugin	Description
Industrial Core	Contains the class mappings needed for the OT Service Graph Connectors. For more information about the Industrial Core plugin, see Industrial Core plugin.

Roles installed

Role	Description
Operational Technology Discovery Administrator [ot_discovery_admin]	Can run the Discovery for Operational Technology process, but cannot access the Configuration Management Database (CMDB) to view the configuration items (CIs) and related Operational Technology (OT) entities that are created from discovered items. To learn more, see Create and run the OT Discovery schedule and the Discovery process.
Operational Technology Manager Viewer [cmdb_ot_viewer]	Read-only access to Operational Technology (OT) device records.
Operational Technology Manager Editor [cmdb_ot_editor]	Create, read, update, and delete access for Operation Technology (OT) extension classes. **Note:** Users assigned the **cmdb_ot_editor** role can edit and delete only OT configuration items (CIs), and don't have the ability to edit IT CIs.
Operational Technology Manager Admin [cmdb_ot_admin]	Create, read, update, and delete access for Operational Technology (OT) device

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role	Description
	records. Can also edit and manage specific configurations in the OT entity type. To learn more, see Operation Technology (OT) extension classes. **Note:** Users assigned the **cmdb_ot_editor** role can edit and delete only OT configuration items (CIs), and don't have the ability to edit IT CIs.

Operational Technology dependencies

The following tables describe the application dependencies required for Operational Technology (OT) device management and OT vulnerability management.

With the full Operational Technology product, you can track and manage your device and vulnerability data within an OT environment. For more information about the applications and features included with the OT product, see the Operational Technology store listing.

OT device management

For a full view of your OT device data and its management, you need the applications and features in the following table.

Note: OT licenses for Operational Technology Service Management (OTSM) apply to OTSM, not ITSM. For more information, see the OT Dependencies [KB3146763] article in the Now SupportKnowledge Base.

Application/Feature	Description
Operational Technology Manager (sn_ot_foundation)	Creates the foundational data and relationships that enable your enterprise to use the Operational Technology Management solution. For more information, see Operational Technology Manager.
IT Discovery for OT Networks (sn_otsm_discovery)	Discovers IT class OT devices. These devices are located in designated Purdue levels within your Industrial Control System (ICS) networks. IT class items include switches, routers, and computers that exist both in data centers and in your factories. For more information, see IT Discovery for Operational Technology (OT) Networks.
OT Enhanced Access Control (sn_ot_enhanced_acl)	Implements data filters, deny unless access control rules (ACLs), and ACL query rules to help improve system security. For more information, see Enhanced Access Control for Operational Technology.
OT Manager Foundation (sn_otm_gen_ai)	Uses generative AI to help streamline processes in the Industrial Workspace related to your OT device data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application/Feature	Description
	For more information, see Operational Technology (OT) Manager Foundation.
OT Asset Management (com.sn_otam)	A specialized offering within the suite of Enterprise Asset Management solutions for managing OT and Operational Equipment (OE) assets. With OT Asset Management, you can effectively manage the lifecycle of OT and OE assets. For more information, see OT Asset Management.
Operational Technology Change Management (sn_ot_chg_mgmt)	Enables your team members to work collaboratively on changes to OT devices or industrial equipment configurations. For more information, see Operational Technology Change Management.
Recommended Actions for Operational Technology Service Management (OTSM) (sn_otsm_ra)	Enables you to set up and apply real-time actionable recommendations for speeding up the triaging process and resolving issues quickly across various records in the Industrial Workspace, including OT incidents. For more information, see Recommended Actions for Operational Technology Service Management (OTSM).
ServiceNow Otto for Operational Technology (OT) Service Management (sn_otsm_gen_ai)	Enables teams to summarize OT incident details and generate incident resolution notes to share with other users. For more information, see ServiceNow Otto for Operational Technology (OT) Service Management.

OT vulnerability management

For a full view of your OT vulnerability data and its tracking, you need the applications and features in the following table.

Application/Feature	Description
Operational Technology Vulnerability Response (sn_otvr)	Enables effective prioritization and remediation of OT device vulnerabilities at the site level. By using the CMDB relationships of OT devices, vulnerable devices or items can be prioritized based on the criticality of the production process they automate. For more information, see Operational Technology Vulnerability Response.
Hardware Vulnerability Assessment (sn_otvr_pro)	Enables you to assess the firmware vulnerabilities of the OT devices in inventory and create vulnerable items (VIT) against the impacted OT devices. For more information, see Operational Technology Hardware Vulnerability Assessment.
Vulnerability Solution Management (sn_vul_solution)	Automates the correlation of vulnerabilities in your environment with the solutions that can remediate them. It identifies the patches,

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Application/Feature	Description
	configuration updates, and controls with the highest impact for your organization, eliminating the need for manual research. For more information, see Vulnerability Solution Management.
Operational Technology Manager (sn_ot_foundation)	Creates the foundational data and relationships that enable your enterprise to use the Operational Technology Management solution. For more information, see Operational Technology Manager.
OT Enhanced Access Control (sn_ot_enhanced_acl)	Implements data filters, deny unless access control rules (ACLs), and ACL query rules to help improve system security. For more information, see Enhanced Access Control for Operational Technology.
OT Manager Foundation (sn_otm_gen_ai)	Uses generative AI to help streamline processes in the Industrial Workspace related to your OT device data. For more information, see Operational Technology (OT) Manager Foundation.

Installed software for Operational Technology Management

The installed software for the Operational Technology Management solution comes from IT Discovery for Operational Technology (OT) Networks or from the OT-certified Service Graph Connectors that support installed software.

Installed software overview

The installed software for a CI varies depending on if you have the Software Asset Management (SAM) application installed. The following tables are created when SAM is activated:

- Software Discovery Model [cmdb_sam_sw_discovery_model]
- Software Model [cmdb_software_product_model]
- Software Installation [cmdb_sam_sw_install]

For more information about how the table structure for managing software installations behaves differently when SAM is activated, see Discovery with Software Asset Management.

You can also configure a computer CI to display Software Asset Management data. For more information, see Configure a CI to display Software Asset Management data.

View installed software for OT devices

You can view the installed software for OT devices in the Industrial Workspace in the following locations:

- The **Software Installed on OT Devices** list by navigating to **All** > **Operational Technology (OT)** > **Software Installed on OT Devices**.
- The **Software Installed on OT Devices** list in the Industrial Workspace list view under the **Operational Technology (OT)** module.
- The **Software Installed** list under the **Related Records** tab in an OT device record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Industrial Core plugin

The Industrial Core plugin contains the class mappings needed for the Operational Technology (OT) certified Service Graph Connectors.

Industrial Core plugin overview

The Industrial Core plugin [sn_ot_core] introduces foundational capabilities to support OT-specific data models and the site based licensing requirements for OT. The plugin is required as a dependency by all products in the Operational Technology Management solution. The dependency can be a direct dependency or a dependency through a base product. For example, the Operational Technology Manager application is a dependency. For the Operational Technology Vulnerability Response application, the Industrial Core plugin isn't added as a dependency because Operational Technology Manager is a direct dependency for Operational Technology Vulnerability Response.

Note: All partner applications integrating with the OT functionality must declare a dependency on the Industrial Core plugin. This ensures consistent handling of licensing and future model enhancements.

Industrial Core plugin features

The following table summarizes the features for the Industrial Core plugin.

Plugin features

Feature	Description
OT Class Mapping Template [ot_class_mapping_template]	The Industrial Core plugin introduces a configuration template to manage class mappings through a user-accessible table part of the OT Service Graph Connectors. This configuration template replaces the prior script-based approach. While the OT Class Mapping Template is currently optional, adopting this method is recommended as it allows you to view, manage, and override class mappings directly in the UI and provides a greater transparency and flexibility. **Note:** Partners can extend the OT Class Mapping Template table in the scope of their application to capture the class mappings specific to the integration. With the OT Class Mapping template, you can also define an OT device naming strategy per class by using the **Allow Custom Device Naming** and **Device Naming Strategy** fields. For more information about how to implement the device naming strategy, see Create and use an OT device naming strategy. For more information about the OT Class Mapping Template and its available fields, see the **OT Class Mapping Template** section

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Plugin features (continued)

Feature	Description
	in Operational Technology (OT) extension classes. For more information about reviewing class mappings for the Service Graph Connector for Microsoft Excel, see Review class mappings.
OT Device Network Connection [sn_ot_device_network_connection]	The OT Device Network Connection [sn_ot_device_network_connection] table references the CI relationships [cmdb_rel_ci] table, and identifies device-to-device connections in CI relationships for OT devices. **Note:** This data is populated with the available OT integrations and cannot be manually created. For more information about the OT Device Network Connection data model, see Operational Technology (OT) extension classes.
OT Site Map [sn_ot_site_map]	The OT Site Map [sn_ot_site_map] table is used to assign metadata information to OT devices and contains the following fields. • Approval group • Assigned to • Change group • Company • ISA assignment site • Location • Managed by • Managed by group • Owned by • Site description • Site name • Network type • Support group • Active • Supported by
OT Discovered Subnet [sn_ot_discovered_subnet]	The OT Discovered Subnet [sn_ot_discovered_subnet] table contains the discovered subnets used for OT subnet mapping and contains the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Plugin features (continued)

Feature	Description
	• CIDR • Discovered managed network • Site
OT Activity [sn_ot_activity]	The OT Activity [sn_ot_activity] table captures the following activities that occur on the OT device: • Addition, update, or retiring of a configuration item • Addition of an IP address
OT Backup Job Execution History [ot_backup_history_and_comparison_log]	The Backup Job Execution History [ot_backup_history_and_comparison_log] class creates a history of records for all backup executions. It compares the history of records for all backup executions.
OT Automation Repo [ot_automation_repo]	The OT Automation Repo [ot_automation_repo] class acts as a repository to store all configuration changes you want to perform on an OT entity.
OT Automation Repo Device M2M [ot_automation_repo_device_m2m]	The OT Automation Repo Device M2M [ot_automation_repo_device_m2m] class acts a reference to the OT Automation Repo and the OT Entity table.
OT AutomationCommit [ot_automation_commit]	OT AutomationCommit [ot_automation_commit] class acts as a reference to the changes you have committed to a project.

Create and use an OT device naming strategy

Create and use the Operational Technology (OT) device naming strategy to create unique names for your OT devices.

Before you begin

Role required: cmdb_ot_admin and script_include_admin

About this task

The Industrial Core plugin comes with the **DeviceNamingStrategyHelper** script include, which identifies whether or not to use the device naming strategy. If yes, then the script identifies which naming strategy to use for a given source class. This helps reduce the number of changes that are required for the Service Graph Connector.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Create an OT device naming strategy.

   a. Switch the **Application scope** from **Global** to the application that you want to create a device naming strategy for.

   b. Navigate to **All** > **System Extension Points** > **Scripted Extension Points**.

   c. Search for and open the **OTDeviceNamingStrategyExtPoint** extension point.

   d. Select the **Create Implementation** related link.
   A script include is created in the application scope you're in.

   e. Update the **Name** field to a unique name that indicates what type of naming strategy the created script defines.

   > **Note:** Ensure you keep the name unique across all Service Graph Connectors as the name is visible in the Class Mapping table form view when you select an existing script from the list of available strategies.

   f. In the **Script** field, implement the **calculateDeviceName** function.
   Make sure the function returns a string value. You have access to the jsonObj parameter, which is an object with information provided by the caller.

   g. Select **Update**.

2. Use an OT device naming strategy.

   a. Switch the **Application scope** from **Global** to the application that you want to make changes for.

   b. Identify the logic where the device name is being calculated.

   c. Initialize the helper script include with your SGC-specific class mapping table name.
   The **OTDeviceNamingStrategyHelpercontains** helper script include contains functions that can identify the correct implementation for the given source class and can calculate the device name.

   d. Prepare the data that's required for the device name to be calculated based on the naming strategy that you defined.
   The calculateDeviceName function expects following parameters.

Parameter	Description
sourceClassName	Source class name. Ensure the name is in the same format as defined in the Class Mapping table.
jsonObj	Any attributes that you want to pass to the implementation. You can use this in the implementation script include.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. Call the **calculateDeviceName** function of the helper script include.

f. Ensure you have a fallback mechanism for calculating the device name.
In cases where there was an error in calculating the device name using the naming strategy, the helper script returns device name as an empty string. Additionally, in a case where no device naming strategy is defined, a default device naming logic is required.

g. Run the device import for your Service Graph Connector to verify whether the changes are working as expected.

Model categories for Operational Technology

When configuration items (CIs) are created in the CMDB, asset records are created. The asset record contains the model category for the CI.

The following table describes the model categories available for Operational Technology (OT) and their CI class.

OT model categories

Name	CI class
Industrial	N/A
Industrial General	Operational Technology (OT) [cmdb_ci_ot]
Operational Equipment	Operational Equipment [cmdb_ci_oe]
OT Control	OT Control System [cmdb_ci_ot_control]
OT Control 3D Printer	Industrial 3D Printer [cmdb_ci_ot_industrial_3d_printer]
OT Control CNC	CNC [cmdb_ci_ot_cnc]
OT Control DCS	DCS [cmdb_ci_ot_dcs]
OT Control DPU	DPU [cmdb_ci_ot_dpu]
OT Control IED	IED [cmdb_ci_ot_ied]
OT Control Module	OT Control Module [cmdb_ci_ot_control_module]
OT Control PLC	PLC [cmdb_ci_ot_plc]
OT Control RTU	RTU [cmdb_ci_ot_rtu]
OT Control SCADA	SCADA Server [cmdb_ci_ot_scada_server]
OT Control Server	OPC Server [cmdb_ci_ot_opc_server]
OT Field Actuator	Industrial Actuator [cmdb_ci_ot_industrial_actuator]
OT Field Device	OT Field Device [cmdb_ci_ot_field_device]
OT Field Drive	Industrial Drive [cmdb_ci_ot_industrial_drive]
OT Field Robot	Industrial Robot [cmdb_ci_ot_industrial_robot]
OT Field Sensor	Industrial Sensor [cmdb_ci_ot_industrial_sensor]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT model categories (continued)

Name	CI class
OT Supervisory	OT Supervisory System [cmdb_ci_ot_supervisory]
OT Supervisory EWS	EWS [cmdb_ci_ot_ews]
OT Supervisory Historian	Historian [cmdb_ci_ot_historian]
OT Supervisory HMI	HMI [cmdb_ci_ot_hmi]
OT Supervisory OPC	OPC Client [cmdb_ci_ot_opc_client]
OT Supervisory SCADA	cmdb_ci_ot_scada_client

APIs for IT to OT and OT to IT conversion

There are 2 APIs used for handling refresh workflow scenarios for converting IT to Operational Technology (OT) and vice versa with the OT Asset Management application.

APIs used in OT Asset Management

With OT Asset Management, you need to maintain synchronization between asset and configuration item (CI) for OT assets. The following APIs are used for IT to OT conversion and OT to IT conversion in the OT Asset Management application.

Note: The IT CI class isn't changed. Instead an OT entity record is added, which provides the OT device context.

- Convert IT to OT Asset API
- Convert OT to IT Asset API

Convert IT to OT Asset API

The Convert IT to OT Asset API is used in refresh workflows where an OT configuration item (CI) is replaced with a new CI. This API creates a replica of the previous OT entity record, and maps them to the new CI. No changes occur in the previous CI and its related OT entity record. Both the new CI and the previous CI references are used with this API.

Convert OT to IT Asset API

The Convert OT to IT Asset API is used if an asset needs to be replaced. The API deletes the OT entity record of the passed CI.

For more information about Asset and Configuration Item (CI) synchronization for Operational Technology (OT) assets, see Asset and Configuration Item (CI) synchronization for Operational Technology (OT) assets.

For more information about OT Asset Management, see OT Asset Management.

Edit the protection policy for an OT View Rule

Edit the protection policy for an Operational Technology (OT) View Rule to edit the View Rule as needed.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System UI** > **View Rules**.
2. To only view the OT View Rules, apply the following filter:
   [Name] [contains] [OT]
3. For the OT View Rule that you want to edit, select the **Read-only** value in the **Protection policy** column.
4. Change the **Protection policy** column value to **--None--**.

Result

Changing the **Protection policy** column value from **Read-only** to **--None--** allows users assigned the **admin** role to edit the OT View Rule.

Related information

Find more information about the Network Intrusion Detection System (NIDS) extension class, OT extension classes, and related applications.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Network Intrusion Detection System (NIDS) CI extension class

The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.

Operational Technology (OT) extension classes

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

CMDB CI Class Models app

The CMDB CI Class Models store app adds class models that extend the CMDB class hierarchy, including class descriptions, identification rules, identifier entries, and dependent relationships.

Operational Technology Discovery

You can use the Operational Technology Native Discovery solution to amplify the visibility of devices in your OT environment. You can also use the IT Discovery for Operational Technology (OT) Networks function to discover IT class OT devices.

Get started

Use these links to explore and learn more about the Operational Technology Native Discovery components or the IT Discovery for Operational Technology Networks.

Explore

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Operational Technology Native Discovery components

IT Discovery for Operational Technology (OT) Networks

Troubleshoot and get help

If you have any errors or difficulties while using the Operational Technology Discovery applications, Contact Customer Service and Support.

Operational Technology Native Discovery components

The ServiceNow® Discovery for Operational Technology (OT) Native components give you visibility of your OT devices. The components import your device data into ServiceNow using the Service Graph Connector for ServiceNow OT Discovery. Using the OT components, that is, the Discovery Console for OT, Discovery Sensor for OT, and OT Discovery Collector, you can monitor and query your devices within the OT environment.

Operational Technology Native Discovery components

Review and install the Service Graph Connector for ServiceNow OT Discovery then install the OT Discovery components. The first component to start with is the Discovery Console for Operational Technology (OT).

Note: For more information, see Service Graph Connector for ServiceNow Operational Technology (OT) Discovery.

Use the links in the Related Topics section to explore the Operational Technology Native Discovery components.

Deploy Operational Technology Discovery

Consider deployment options for your Operational Technology Discovery components.

Where to start

You can use the links in the Related Topics section to consider and learn more about deploying the Operational Technology Discovery components.

Architectural considerations

This document intends to describe the ServiceNow Operational Technology Discovery architecture and covers how discovery components find, identify, and inventory devices in an Operational Technology environment.

Operational Technology Discovery software architecture

Today's industrial environments are made up of hundreds — sometimes thousands — of connected devices: programmable logic controllers, remote terminal units, human-machine interfaces, protection relays, and more. Tracking all of them — what they are, where they sit in your network, and whether they behave as expected — is a foundational challenge of operational technology.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following describes the software architecture underlying the ServiceNow Operational Technology Discovery platform.

How Discovery works

At its core, Operational Technology Discovery actively reaches out to devices on your network using the same protocol language those devices already speak. Each device receives a query in its native protocol and responds with identifying information. A Modbus device gets a Modbus query. An EtherNet/IP device gets an EtherNet/IP query. This approach avoids aggressive network scanning that can disrupt sensitive industrial equipment.

The result is an updated inventory of your OT environment, visible through a single interface and integrated directly into your broader IT service management platform.

Note: The user sets the protocol parameters for the query from the Discovery Console for OT.

Active Discovery approach

Before exploring how the discovery components work in detail, it helps to understand the Operational Technology Discovery uses an active discovery approach.

The **Active** discovery initiates communication directly with devices using their native industrial protocol language — sending the same kinds of queries an engineering workstation or HMI would send to a PLC. These queries are indistinguishable from normal operations. Devices can't distinguish these queries from regular engineering traffic, making properly implemented active discovery safe for operational networks.

Active discovery is easier to setup and start because it can require a Console and a single Sensor or Collector rather than a distributed set of SPAN ports and collection devices.

The key advantage of active discovery is coverage. Because it reaches out to devices rather than waiting for them to communicate, it can detect silent and dormant assets that passive monitoring would never see. It also retrieves granular details — firmware versions, serial numbers, configurations — that may never appear in normal network traffic.

The Discovery components

The architecture is built around three components that work together. It is important to understand each component's distinct role and responsibilities.

The Discovery Console for OT is the interface you use to configure discovery, define the areas of your network you want to scan, and view the results. You can place more than one Console in your network.

- The Console is your starting point. It is where you define your industrial sites, configure the network zones and sites you want to discover, and set up the queries that drive the process. After discovery is running, the Console is also where you view results — seeing your OT environment take shape as devices are identified and cataloged.
- In terms of network placement, the Console typically, but not necessarily, sits in an IT/OT DMZ or a dedicated secure management zone. It doesn't perform discovery itself, but it configures the Sensor and serves as the central point of visibility across your entire deployment.

The Discovery Sensor for OT does the discovery work. Deployed as software on a virtual machine or physical server, the Sensor reaches out to devices in your network, identifies them, and builds your device inventory. It does this actively — on a schedule you configure. You can place Sensors throughout your network.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Sensor does the active discovery. Deployed as software on a virtual machine or bare metal system, it executes the queries configured in the Console. It builds your device inventory from the responses it receives. When the Sensor queries a device, it uses that device's native industrial protocol — Modbus, DNP3, EtherNet/IP, and others. This keeps the interaction safe for the network. You can select the protocol for the query in the Console.
- However, industrial environments are often deeply segmented by design — and the Collector addresses this.

The OT Discovery Collector extends the Sensor's reach into parts of your network that the Sensor can't access directly. In large or highly segmented industrial environments, a single Sensor may not have network visibility into every zone. Collectors are lightweight components deployed within those zones to bridge the gap. You can also use more than one of these components in your OT environment.

- The Collector is a (small) application that can be installed on exiting systems (for example, HMIs) to extend discovery.
- Combined with the Sensor, it offers flexible deployment options to assist with maximum coverage of the OT network.

The Discovery workflow

It is easier to understand how the three components work together when you follow a discovery job from start to finish. The following covers that process — from building a query in the Console through to a fully populated device inventory in the ServiceNow instance.

Step 1: The network is built with Discovery in mind

Before any discovery runs, the Consoles, Sensors, and Collectors are deployed at positions in the network that reflects the user's OT environment. There are no fixed rules about how many OT components are needed to deploy or exactly where to place them. This depends on your OT network.

Sensors and Collectors are deployed to cover the network. They can be deployed on bare-metal hardware or on a Virtual Machine, depending on what suits each part of the network. The Console, however, is recommended to run on a Virtual Machine. Discovery can return photographic data alongside standard device attributes. A Linux distribution should be installed on the same VM before the Console is installed.

Step 2: Build a query in the Console.

Discovery begins when you create a query in the Console, where you define exactly what you want to discover and how. Query parameters include:

- **Protocols**: Which industrial protocols to use when communicating with devices, such as Modbus, DNP3, or EtherNet/IP.
- **Brands**: Filtering discovery toward specific device manufacturers if needed.
- **Ports**: Which network ports to include in the query.
- **Assets**: Which devices or ranges of devices to target.
- **Sites**: You can create or discover sites.
- **Query type**: Simplified and advanced query types such as the OPC-UA type, which captures photographic and visual data from devices rather than relying solely on protocol-based communication.

You can also select specific Sensors and Collectors the query should use. Because Sensors and Collectors are deployed at known positions in the network, you can pick specific components

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

by name — choosing the Sensor inside Line #1, for example, because you know that's where the devices you want to discover are located. Alternatively, you can let the query use the appropriate components based on where they are positioned in the network.

Step 3: The query runs through the selected components.

Once configured and launched, the query drives everything. Each Sensor and Collector executes the query within its part of the network, reaching out to devices using the protocols and parameters the user defined. A Sensor handles discovery in the zones it can directly access. A Collector does the same in the deeper or more restricted zones where it has been positioned.

Because both Sensors and Collectors are independently deployed and selectable, a single query can span multiple zones simultaneously. The Sensor handles one part of the network and the Collector handles another, all driven by the same query configuration.

Step 4: Results upload to ServiceNow.

As devices respond, their details are collected and returned to the Console. These include device type, vendor, model, firmware version, network address, zone, Purdue level, and where applicable, photographic data. From the Console, the data is uploaded to the ServiceNow instance.

Note: It should be noted that depending on your network structure, there are additional OT components used to reach the ServiceNow instance, if needed. For further information on OT Discovery connections, see the OT Discovery deployment scenarios or the Service Graph Connector for ServiceNow OT Discovery Guided Setup.

Within the ServiceNow instance, discovered devices are mapped to configuration items predefined in the CMDB. These configuration items are based on industry and operational device types, reflecting the OT world your team works in every day. They can be edited and adjusted to fit the data retrieved, giving your team flexibility to tailor the inventory to your environment.

The result is an accurate, up-to-date inventory of your OT environment — built through the discovery components your company has positioned in the network. It is visible through a single interface and integrated directly to ServiceNow without manual surveys or spreadsheets.

Wrapping up

Operational Technology Discovery is built on the principle that visibility should not come at the cost of safety. By deploying the Console, Sensor, and Collector at deliberate positions within your network — and querying devices in a way that is safe for operational environments — the system adapts to your environment rather than requiring you to adapt your environment to it. Whether you're managing a single compact site or a large enterprise with dozens of segmented zones, the architecture scales accordingly. The result is a current, accurate inventory of your OT environment, fully integrated into ServiceNow and built without disrupting the operational processes your network supports.

Before deploying OT Discovery

To discover assets in your OT environment, the Operational Technology Discovery solution provides the ServiceNow platform, the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector.

Before you deploy

Consider these questions before planning your Operational Technology Discovery deployment. This list is not exhaustive.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Are you looking at OT devices or IT devices in the OT network?
- Have you planned the Site location?
- What is the network layout and architecture of the Site location? Is it a flat or segmented layout?
    - The best way to start is to place a Discovery Sensor for OT in a location that includes many of the devices to be queried.
    - Next, place additional Sensors in areas of the network that might have segmentation or other barriers, such as a NATed environment or segmented silos.
- Are there any network zones in place? Identify any NATed networks or copy-paste networks (sites with identical IP ranges).

    Note: When Sensors can reach the same zoned location or when assets are dual-homed, carefully document the zoned Sensor configuration to avoid creating duplicate asset records.

- What communication pathways exist within the site?
- If Sensors are deployed in each Network (NW) zone, can they communicate with the assets in the OT network?
- Do any other devices have to be installed?
- Where does the Discovery Console for OT get installed?
- Can one Console be used for multiple sites or does the deployment require one Console per site?
- Are there communication paths between the Sensors and the Console?
- Does the MID Server exist in DMZ?
- Is there a communication path between the Console and the MID Server?
- Are there any other tools (IDS or Discovery tools) in the OT environment?

Adding capabilities over time

With OT Discovery, you can add layers of capabilities over time such as:

- Deploying the Discovery Console for OT and Discovery Sensor for OT in a central location with access to multiple sites.
- Deploying the Discovery Sensor for OT at individual sites, with additional Sensors deployed as needed for policy enforcement or non-IP-enabled asset monitoring.

Adding locations over time

On a site-by-site level, you can add locations over time, such as deploying the Discovery Console for OT and the Discovery Sensor for OT at a pilot site. For more information, see the Sites page.

OT Discovery System Resources

You can review the OT Discovery component resources before setting up your OT network.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Discovery components required resources

The requirements in this section are a generalization. Consider factors such as segmentation level, communication pathways, network traffic, redundancy, and environmental conditions. Also account for physical constraints when determining network requirements. The following tables provide resource estimates for each OT Discovery component. Review your system requirements beyond these minimums.

Discovery Console for OT System requirements

Component	Minimum System Requirements
Discovery Console for OT	• 16 GB RAM • 100 GB Hard drive • 2 CPUs

For additional requirements for the Console, see Requirements for Discovery Console for OT installation and Install the Discovery Console for Operational Technology (OT).

Discovery Sensor for OT System requirements

Component	Minimum System Requirements
Discovery Sensor for OT	• 2 GB RAM* • 100 GB Hard drive • 2 CPUs • 2 virtual NIC cards *8 GB of RAM is recommended for all queries.

For additional requirements for the Sensor, see Configure the Discovery Sensor for OT.

Note: The Collector can be installed and run on either a Windows OS or a Linux OS.

OT Discovery Collector minimum system requirements

Component Operating System	Minimum System Requirements
Windows	The OT Discovery Collector installation is compatible with Windows 10 or Windows 11 systems. The required Windows (10 or 11) environment for the OT Discovery Collector is x86_64. ARM or Apple Silicon devices aren't supported. See Install the OT Discovery Collector on a Windows system.
Linux	See Install OT Discovery Collector on a Linux system for specific information.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Discovery communications

This section describes how the OT Discovery components should be connected so they can communicate with each other.

Component communications

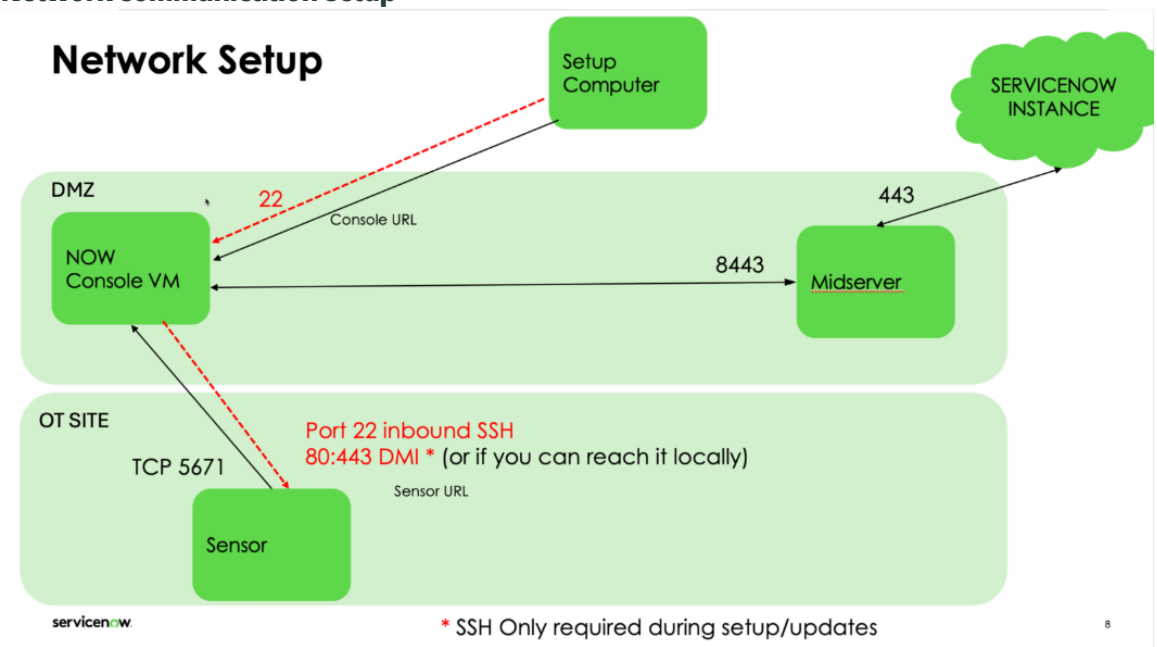
When determining the environment architecture for your deployment, consider how the following OT Discovery components interact.

- MID Server-to-ServiceNow instance:
  - The MID Server needs to communicate with the ServiceNow instance to push the information from Discovery Console for OT.

    Note: If the Discovery Console for OT can reach the internet, the MID Server might not be needed in your OT configuration.

  - This configuration and deployment is the same as with any other MID Server.
  - The Service Graph Connector (SGC) needs to communicate with the MID Server, the Console, and the ServiceNow instance.
- Console-to-MID Server communication:
  - Deploy a separate MID Server for each network or network segment.
  - Configure firewall rules to enable communication across networks or network segment boundaries.
  - The Console needs to communicate with the Sensors, the Collectors, the MID Server, the SGC, and your ServiceNow instance.

Network communication setup



- Sensor-to-Console communication:
  - Deploy a separate Console for each network, network segment, or system.
  - Configure firewall rules to enable communication across networks or network segment boundaries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Discovery Sensor for OT needs to communicate with OT assets and with the Discovery Console for OT.
- Discovery Sensor for OT data is pushed to the ServiceNow instance by the Service Graph Connector.

- Sensor-to-asset communication:
  - Deploy a separate Sensor for each network, network segment, or system.
  - Configure firewall rules to enable communication across network, network segment, or system boundaries.
- Discovery OT Collector-to-Console communication:
  - Discovery OT Collector needs to communicate with the Console.
  - The Collector communicates with the Console and with your system's assets.

Network port map

The following table describes how to set up network ports.

Network port map

Source	Destination Port	Direction	Destination	Required/ Optional	Description
Management Console	8443 (HTTPS) inbound	Bi <->	Workstation	Required	Console web interface
Management Console	5671 (AMQP) inbound	Uni <-	Sensor	Required	Communications from Sensors to Console
Management Console	123 (NTP) inbound	Uni <-	Time Server / Esxi Host	Optional	Clock synchronization, Not needed it time server or hypervisor will provide time.
Management Console	8443 API	Uni <-	MID Server	Required	Import data from Management Console via the APIs.
Management Console	22 (SSH) inbound	<-	Host Setup Computer	Optional (setup)	Additional support during deployment
Sensor	5671 (AMQP) outbound	Uni <-	Management Console	Required	Communications from Sensors to Console
Sensor	443 (HTTP) inbound	<-	Host Setup Computer	Required	Additional support during deployment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Network port map (continued)

Source	Destination Port	Direction	Destination	Required/ Optional	Description
Sensor	22 (SSH) inbound	<-	Host Setup Computer	Required	Additional support during deployment
MID Server	443	Bi <->	NOW instance / Web	Required	Communications from the MID Server to the NOW fabric internet facing.

OT Discovery deployment scenarios

Deployment scenarios for OT Discovery vary based on a network's architecture. Use these scenarios to help determine how to deploy the OT Discovery components in your OT environment.

Note: The OT Discovery Collector can be deployed to the same locations as the Discovery Sensor for OT.

General recommendations

General recommendations and guidance are listed in each scenario in these sections. Not all networks are the same. The requirements in this section are a generalization for the scenario. Consider factors such as segmentation level, communication pathways, network traffic, redundancy, and environmental conditions. For resource recommendations for the OT Discovery components see, OT Discovery System Resources.

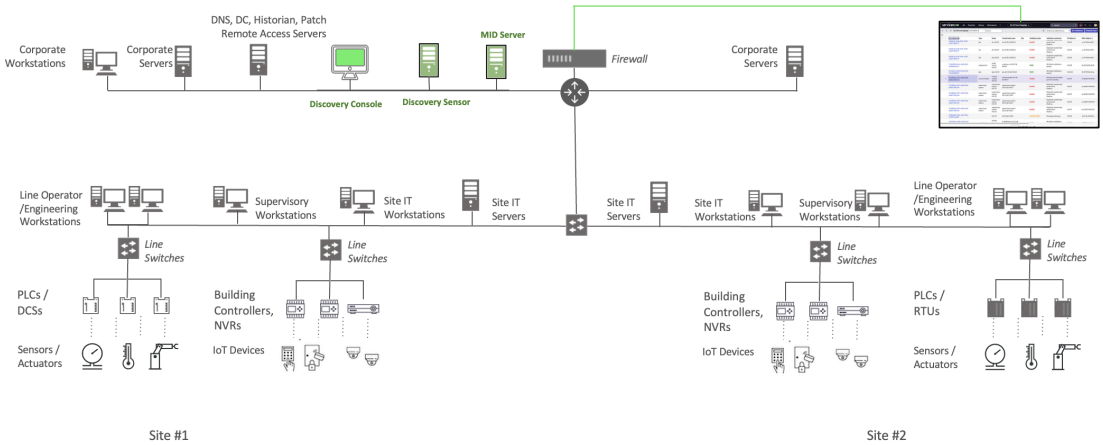
Flat network architecture across multiple sites

A flat network architecture is a network design that has all available Discovery Console for OT, Discovery Sensor for OT, and OT Discovery Collector connected to a single network, where the Sensors and Collectors can communicate with each other directly.

You can have one or more sites that communicate with each other.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Flat network



The Console, Sensors, and MID Server connect at Purdue level 3.5 and push data through the switches and the firewall to the ServiceNow instance for ingestion.

Components in the flat network

The following are the components in a flat network.

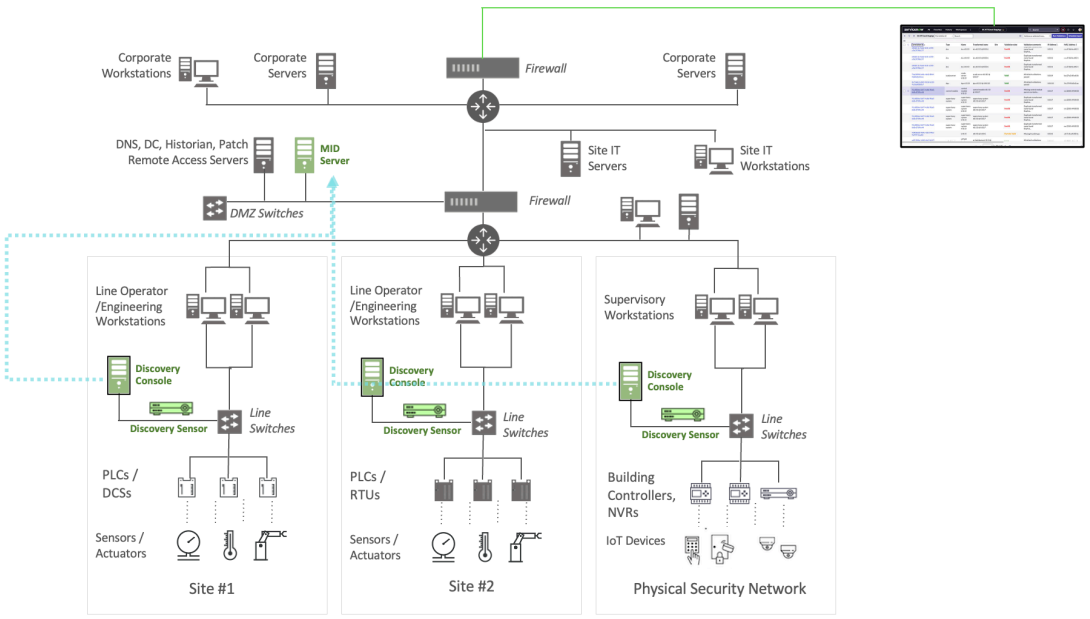
- Discovery Console for OT and Discovery Sensor for OT.
- A localized appliance or VM that serves as the command-and-control interface for asset discovery and communication in its respective segment. This appliance or VM manages credentials, protocol handlers, and initiates querying operations locally. In such a scenario, a typical deployment means that one Console covers multiple sites.
- Deploy the Console at a layer where the MID Server can connect to the Console and the ServiceNow instance.
- Deploy Sensors based on the desired speed of the discovery. In a truly flat network, a Discovery Sensor for OT can reach all the OT assets in that network. More Sensors in the network can help improve the speed of discovery.

Multiple independent segmented sites

A segmented site architecture is a network design that has the network split into multiple segments. Each segment contains its own Discovery Console for OT and multiples of the Discovery Sensor for OT and the OT Discovery Collector. There is no communication between sites. Each of the segments could be considered a flat network.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Segmented sites



In this OT environment, the network is segmented into three distinct zones for operational clarity, security, and control:

- Site 1 Operational Technology segment
- Site 2 Operational Technology segment
- Physical Security Network segment

Each segment contains its own isolated infrastructure to reduce risk and increase visibility in its respective domain. Components in each segment:

- Discovery Console for OT or VM that serves as the command-and-control interface for asset discovery and communication in its respective segment. It manages credentials, protocol handlers, and initiates scanning operations locally.
- Discovery Sensor for OT is deployed in each segment. The Sensor performs active discovery, collects network traffic, and queries for known protocols (for example, Modbus, DNP3, BACnet). It reports findings to its segment's Console.

The Consoles and Sensors are deployed in their respective network zones and don't have direct outbound access to the internet.

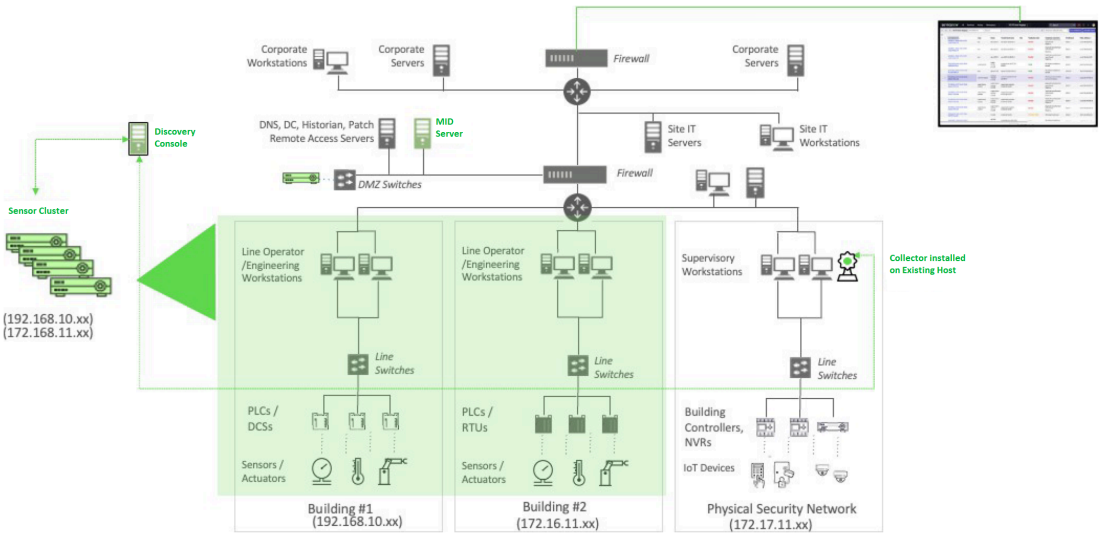
Micro-segmented site with multiple networks

A segmented site architecture with multiple networks is a network design that has more than one network split into multiple segments. Each segment contains multiple network segments and its own Discovery Console for OT and Discovery Sensor for OT.

- Make sure the Sensors and Collectors have a communication pathway to the Console.
- Deploy Sensors in each segment where the Sensor can perform active discovery in the segment and collect network traffic and can scan or query for known protocols (for example, Modbus, DNP3, BACnet). It reports findings to its segment's Console.
- If you use an existing host to do the discovery in the network such as Human Machine Interface (HMI) or Engineering Workstation (EWS), you can install the OT Discovery Collector to perform discovery.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Segmented site with multiple networks



Discovery Console for Operational Technology (OT)

Use the Discovery Console for OT component to discover, monitor, and query devices in your Operational Technology environment.

Get started

Use the links in the Related Topics section to explore, configure, and learn more about the ServiceNow Discovery Console for OT.

Explore the Discovery Console for Operational Technology (OT)

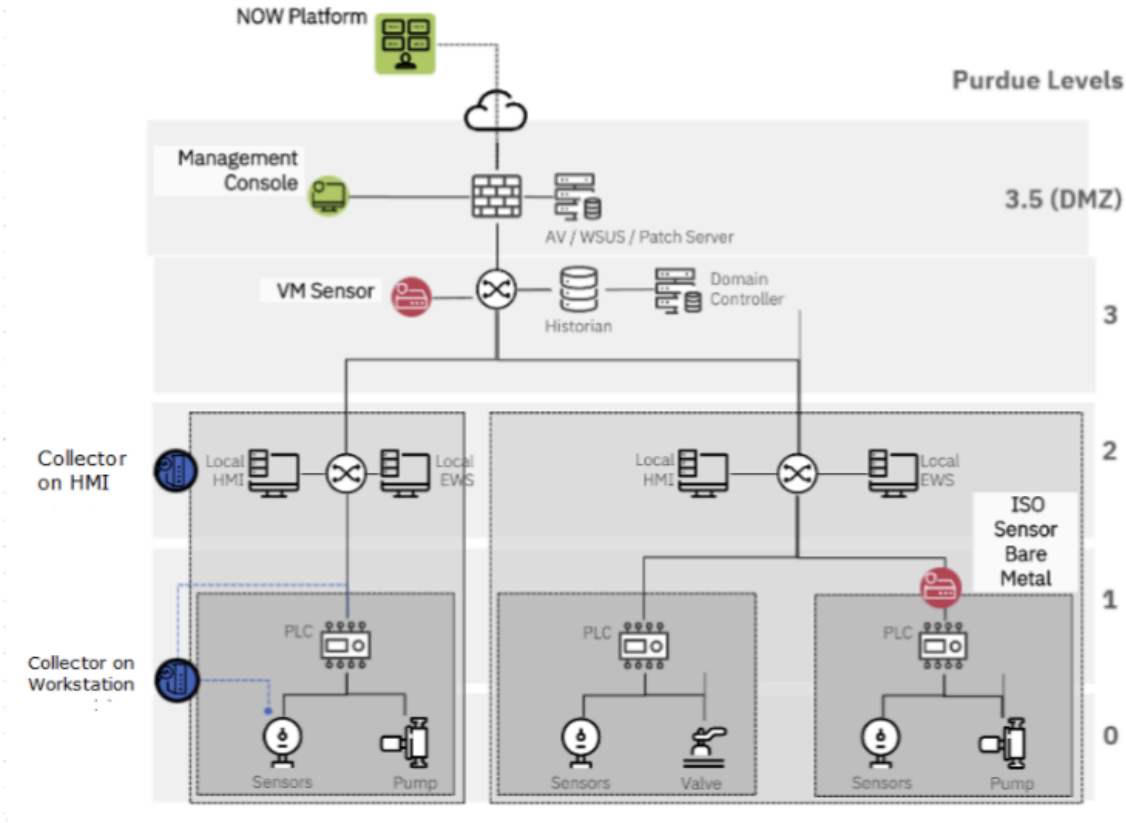
The Discovery Console for OT provides you with enhanced features to discover your assets in the OT environment.

Discovery Console for OT Overview

The Discovery Console for OT provides complete operational technology visibility across your entire OT environment. This awareness starts at the Human Machine Interface (HMI Purdue Reference Model Levels 2 and 3) and goes down to the field devices (Level 0) through the Discovery Console for OT Network and Sensors. From the Discovery Console for OT you can enable and configure device management capabilities. The Discovery Console for OT and Discovery Sensor for OT work together to create a comprehensive device inventory that you can monitor and manage from a single interface.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Purdue levels



Discovery Console for OT uses and benefits

Some of the uses and benefits of the Discovery Console for OT are as follows.

- Uses
  - You can use the Console as a configuration manager for your OT devices.
  - Configure schedules, manage sites, networks zone, configure discovery settings, review the asset data, and provide access to additional users.
  - You can manage and monitor several Discovery Sensor for OT and OT Discovery Collector components.
- Benefits
  - Acts as a single source of truth for all OT Devices discovered in the Sites.
  - The Console manages OT assets and provides visibility to OT operators.\

Accessing the Discovery Console for OT

Access to the Discovery Console for OT requires these steps:

Note: Before you can use the Console, you must have a license. Request a Console license from your ServiceNow account representative.

1. Have an active ServiceNow® instance.
2. Go to the ServiceNow Store, acquire and install the Service Graph Connector for ServiceNow OT Discovery, and navigate to the SGC Guided Setup page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. The first step of the Guided Setup is to select the link to the **Download & Deploy** for the OT Discovery components.
4. From there, download the installation packages for the Console, Sensor, and Collector, as desired.

   Note: It's recommended that you install the components in this order: Console, then Sensor, and then Collector.

5. The Console installer packages must be installed on a virtual machine with a Linux distributed OS.

Use the Discovery Console for OT interactive configuration wizard

The Discovery Console for OT provides an interactive configuration wizard that steps you through setting up your Console, Sensor, Collector, assets, queries, and sites.

Before you begin

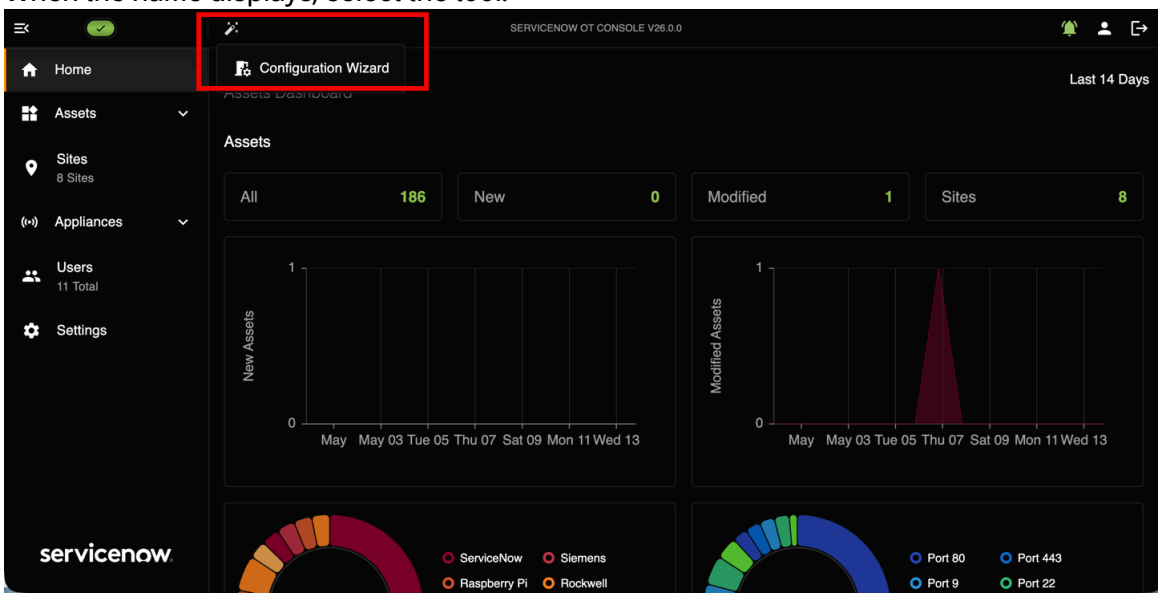
Role required: admin

About this task

After you have installed and setup the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector on your system, the Console's interactive configuration wizard is available for use. The wizard steps through the initial tasks for using the Console, setting up Sensors and Collectors, and gives you an overall introduction to using the OT components.

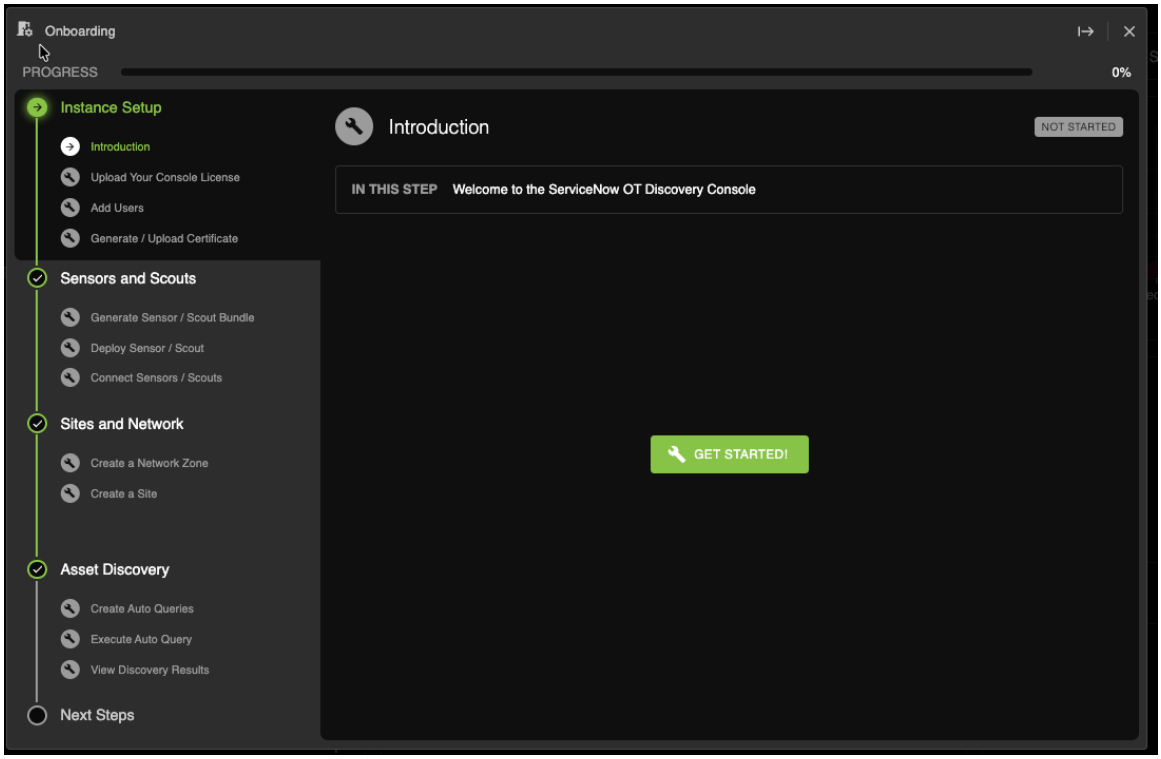
Procedure

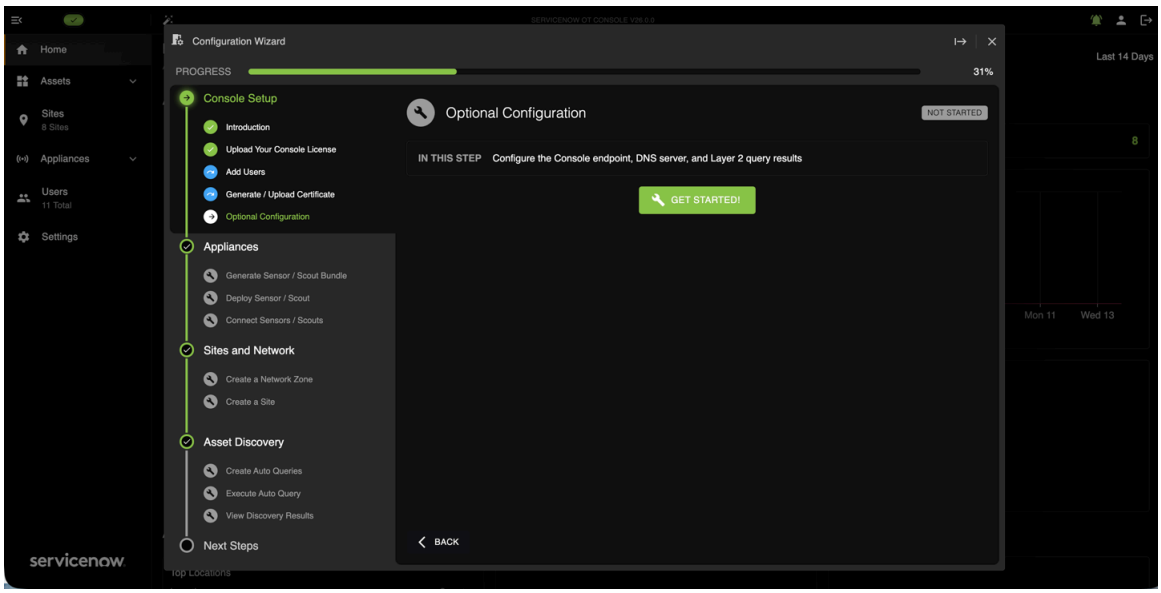
1. On the Console **Home** page, select the wand at the top of the page (Tools).
2. When the name displays, select the tool.



3. The configuration wizard opens in the Console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



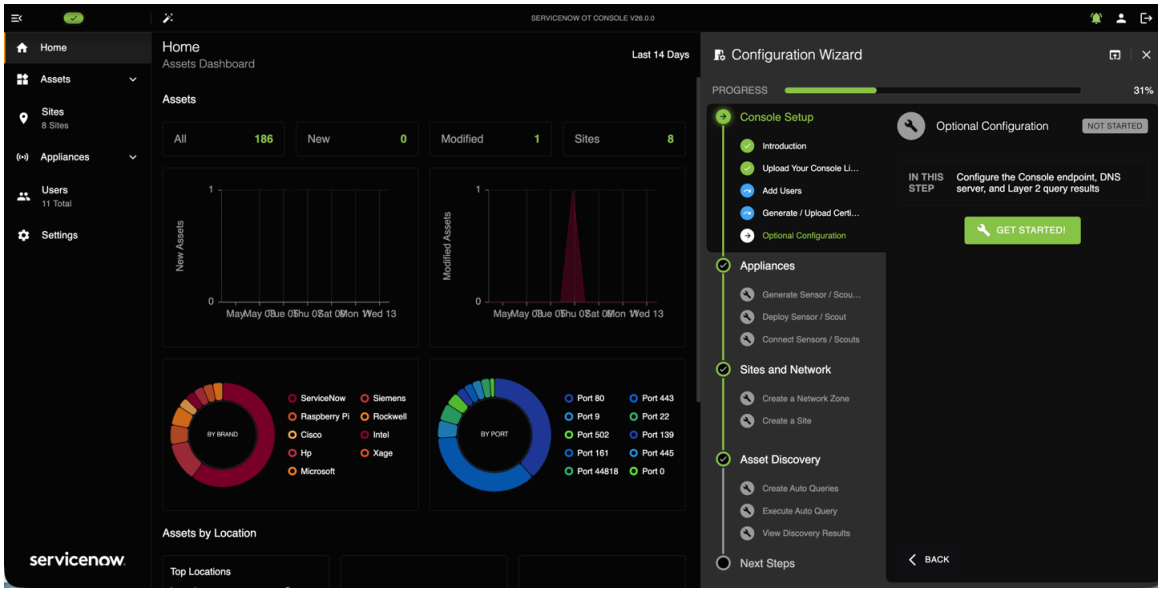


4. You can collapse the wizard to the right side of the Console screen by selecting the icon in the top, right corner of your screen.

   Move the wizard to the right (collapse) to improve Console visibility.

   To expand and center the wizard on the screen, select the icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. The wizard steps you through tasks such as configuring your Console, connecting the Sensor and Collector, creating a site, and creating Auto Queries.
6. Just follow the steps in the wizard and when you complete each one, mark them as **Done**.
7. The wizard provides a **Skip** button so you can skip any of the optional steps.
8. You can open the configuration wizard on any Console page by selecting the **Tool** wand.

Configure the Discovery Console for OT

This section is an overview of the steps for installing the Discovery Console for OT.

Note: During the installation of the non-containerized version of Discovery Console for OT, you must have access the internet to download and install dependent third-party packages such as MongoDB and RabbitMQ. The Console installation automatically installs these packages as long as there's an internet connection. After installation of the third-party packages, the internet connection is unnecessary.

Workflow

In your instance, navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup page and select Get Started. In the top section, select the Download & Deploy OT Discovery link. The Download & Deploy OT Discovery page opens. Select **Configure** and the Downloads page opens. Download the OT component packages.

Note: The required dependency version has been changed to .NET 10 from .NET 8

Review the steps in the installation process listed in the Installation Workflow table.

Discovery Console for OT Installation Workflow

Task	Description
Install virtual machine	You can use any type 1 or type 2 hypervisor. For example: • VMware • Hyper-V • Azure

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Discovery Console for OT Installation Workflow (continued)

	• AWS • Google Cloud • Proxmox
Install Linux distribution on the VM.	Install Linux or install a compatible Linux distribution such as: • RedHat Enterprise Linux (RHEL) 8.x, 9x, and 10x • Rocky 8.x, 9x, and 10x • Debian 12 and 13 • Ubuntu 22.04 and 24.04
Hardware requirements	• RAM: 16 GB (Recommended) • Hard Disk drive: 100 GB • CPUs: 2 For more information, see OT Discovery System Resources.
Connection	Confirm that you have access to the ServiceNow instance.
Installation packages	As previously stated, from the Downloads page, download the Discovery Console for OT, Discovery Sensor for OT, and the OT Discovery Collector packages.
Containerized packages	For closed network systems, you can download and install containerized packages for the Console and the Collector. Select the Collector package that is compatible to your machine's OS. For more information, see Air-gapped networks and OT Discovery installation.
Begin the install for the Discovery Console for OT	Install the Discovery Console for OT before you install the Discovery Sensor for OT. Install the OT Discovery Collector last.
Move the package into the VM	Move the Console installer package into the VM.
Extract the installer	From the Console package, extract the ConsoleInstaller .ZIP file.
Run the installation script	Execute ./console-init.sh. This script confirms all the required components are installed. **Note:** If you're using the traditional console package (that is, non-containerized package) you need access to internet to download dependent third-party packages such as MongoDB and RabbitMQ.
Accessing the web console	To access the web console UI, open the browser and navigate to https://<IP address of the console VM>:8443.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Discovery Console for OT Installation Workflow (continued)

Register initial user	Before you can log in to the Console for the first time, you must register as a user. In the log in window: **1.** Enter your username and an email. **2.** Create your own password or generate a random password. **3. Copy and save this password.** **4.** Enter the password. **5.** Select the check box, **I acknowledge I saved my password**. **6.** Select **Enter**. **Note:** Make sure to save the password, to avoid getting locked out of the system. For more information, see Log on to the Discovery Console for OT.
EULA Agreement	Next, the EULA appears on the screen. Accept the EULA by checking the box next to **Agree**.
Generate a new certificate	After the Console is installed, generate a new Console certificate. For more information, see Generate a certificate.

Note: Once installation is complete, and you log in to the Console, you can choose to use the interactive configuration wizard. The wizard guides you to upload your Console license. It also takes you through the getting started with the system, such as: creating a Site, creating a Network Zone, and building your initial Auto Query. For more information, see Use the Discovery Console for OT interactive configuration wizard.

Air-gapped networks and OT Discovery installation

This section explains the options for air-gapped and non-air-gapped network, installation of Discovery for OT components, and accessing data from scans and queries.

Non-air-gapped networks

During the installation of the Discovery Console for OT, you must have access to the internet to download and install dependent third-party packages such as MongoDB and RabbitMQ. The Console installation automatically installs these packages as long as there's an internet connection. After installation of the third-party packages, the internet connection is unnecessary.

When using the installation for a non-air-gapped network, the Discovery Console for OT not only needs access to dependent third-party packages, but it also needs to communicate with the Sensors, the Collectors, the MID Server, the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery, and your ServiceNow instance.

For these specific steps see the documentation on configuring the individual OT Discovery components. Start with Configure the Discovery Console for OT.

Air-gapped networks

If you plan to install the Discovery Console for OT on an air-gapped network, additional steps are needed to move your queried data from your OT components and environment to your ServiceNow instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

One way to work around this type of network is to first install the OT Discovery component packages on your network. The challenge is then how to get the data from your network to the Mid Server so that it is uploaded to the ServiceNow instance. To do this:

1. Run queries within your closed network with the OT Discovery components to generate the desired data.
2. Download the physical data files from the Console to a physical, portable storage device (USB drive).
3. Then manually move these files to the MID Server.
4. On the MID Server, create a folder for your files.
5. Copy the physical files to this folder on the MID Server.
6. The MID Server uploads your data to your ServiceNow instance.

What to do next

For more information, see Install containerized OT Discovery packages.

Install containerized OT Discovery packages

Install the OT Discovery containerized packages on your network.

Before you begin
Role required: admin

About this task
To help meet the air-gapped challenge, ServiceNow provides containerized versions of the Discovery Console for OT and the OT Discovery Collector. The Discovery Sensor for OT package has everything it needs and can be installed as is to an air-gapped network. The following steps cover installation of the containerized Console and Collector packages.

Procedure

1. On your ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page.
2. Select **Get Started**.
   The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.
5. Read the End User License Agreement (EULA) carefully and then check **Agree**.
6. Download the containerized OT Discovery dependencies package and the installer package.

   Note: Download the OT Discovery Collector containerized package that is compatible with your machine's OS.

7. Decompress the downloaded packages.

   Note: In case you're installing on a Debian OS, install Docker for Debian OS. For more information, see Install Docker Engine on Debian

8. Set up the latest version of docker:

```
sudo apt install docker-ce docker-ce-cli containerd.io
 docker-buildx-plugin docker-compose-plugin
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Run the `build-rabbit-and-mongo-images.sh`.

```
chmod +x build-rabbit-and-mongo-images.sh
 ./build-rabbit-and-mongo-images.sh
```

This builds the containers for RabbitMQ and MongoDB.

10. Copy the RabbitMQ and MongoDB containers into the `OCI_compliant_images` directory.

```
sudo cp offline-console-mongodb_latest.tar.gz
 offline-console-rabbitmq_latest.tar.gz
/home/serviceadmin/OfflineConsoleInstaller/OCI_compliant_imag
es/
```

11. Copy the RabbitMQ and MongoDB containers into the Installer folder.
12. Install Podman:

```
sudo apt install podman podman-compose
```

13. Install the offline console:

```
chmod +x offline-console-init.sh
./offline-console-init.sh
```

Install containerized OT Discovery components on Rocky 10

Install the containerized packages for the Discovery Console for OT and the OT Discovery Collector onto a machine with Rocky 10 OS.

Before you begin

Role required: admin

Procedure

1. On your ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page.
2. Select **Get Started**.
   The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure**.

   The **Downloads** page opens.

   Note: Review the End User License Agreement (EULA) and select **Agree** before proceeding. Consider moving these actions to separate steps.

5. Download the containerized OT Discovery dependencies package and the installer package.

   Note: Download the OT Discovery Collector containerized package that is compatible with your machine's OS.

6. Decompress the downloaded packages.
7. Run the `Build the Offline Installer` script.
   This creates a ZIP archive that contains an offline installer that can be used in air-gapped networks.
8. After the installer is complete, move the ZIP archive to the target system for installation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Decompress the offline installation archive.
10. Copy the required files:

```
scp -r offline-console-init-support-files-main
 serviceadmin@<Console IP Address>:/home/serviceadmin
```

```
scp -r OfflineConsoleInstaller serviceadmin@<Console IP
 Address>:/home/serviceadmin
```

```
serviceadmin //@<password>
```

```
ssh serviceadmin@<Console IP Address>
```

11. Install Podman:

```
dnf install -y zip podman
```

12. Set up the latest version of Docker:

    a. Update system:

    ```
    sudo dnf update -y
    ```

    b. Install the dnf plugins package, which is required for config-manager:

    ```
    sudo dnf install -y dnf-plugins-core.
    ```

    c. Add the official Docker repo: .

    ```
    sudo dnf config-manager --add-repo
     https://download.docker.com/linux/centos/docker-ce.repo
    ```

13. Install Docker.

```
sudo dnf install -y docker-ce docker-ce-cli containerd.io
 docker-buildx-plugin docker-compose-plugin
dnf install -y which
```

14. Unzip the Discovery Console for OT dependencies package and build the containers for RabbitMQ and MongoDB:

```
chmod +x build-rabbit-and-mongo-images.sh
./build-rabbit-and-mongo-images.sh
```

15. Copy the RabbitMQ and MongoDB containers into the Installer folder:

```
sudo cp offline-console-mongodb_latest.tar.gz
 offline-console-rabbitmq_latest.tar.gz
/home/serviceadmin/OfflineConsoleInstaller/OCI_compliant_imag
es/
```

16. Install the offline console:

```
chmod +x offline-console-init.sh
./offline-console-init.sh
```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Requirements for Discovery Console for OT installation

For remote deployment at a facility or on a network, verify that the following requirements are met before installing the Discovery Console for OT.

Infrastructure requirements

You must have a Linux operating system installed that can operate in a virtualization environment or on a Bare-metal server. Install the Discovery Console for OT on a virtual machine.

Note: After installing the Console and the Operating System (OS) on a virtual machine (VM), the VM must have a minimum of 10-GB of unused space available.

System requirements

The table lists the minimum resource requirements for the Discovery Console for OT. For more information, see OT Discovery System Resources.

System Requirements

Component	System Requirements
Discovery Console for OT	• 16 GB RAM • 100 GB Hard drive • 2 CPUs

Note: The required dependency version has been changed to .NET 10 from .NET 8

Network requirements

The Discovery Console for OT requires the following ports to be open inbound (from the connection source to the Console) to operate.

Network requirements

Ports	Description
TCP 5671	Used by Discovery Sensor for OT to communicate with the Discovery Console for OT. This port is used by the Sensor to report data and receive configuration updates from the Console.
TCP 8443	Used to connect to the Discovery Console for OT Web interface. This port is used by the API.
TCP 5002	Enables Sensors to communicate with the Discovery Console for OT to receive updates.
TCP 443	Used for network communication from the Console to a ServiceNow instance or MID Server via the Service Graph Connector for OT Discovery.
UDP 123 (Required)	Enables Sensor devices to synchronize time (real-time clock) with the Discovery Console

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Network requirements (continued)

Ports	Description
	for OT to verify that the time associated with reported data and events is both precise and accurate. **Note:** Without port UDP 123 open on the firewall, the clocks of Sensors drift apart from the clock of the Console. When clock drift is present, various features that rely on precise clock synchronization don't work as expected.

Note: If there are problems accessing the Discovery Console for OT, check the firewall rules and unblock the specific IP addresses and ports used for the installation. If you have any errors or difficulties while using the Discovery Console for OT, contact Customer Service and Support

Discovery Console for OT configuration wizard

The Discovery Console for OT now provides a configuration wizard to guide you through your initial setup and configuration of the Console. If you choose to use the interactive configuration wizard after logging into the Console, it alerts you automatically to upload a Console license. For more information, see Use the Discovery Console for OT interactive configuration wizard.

Discovery Console for OT license

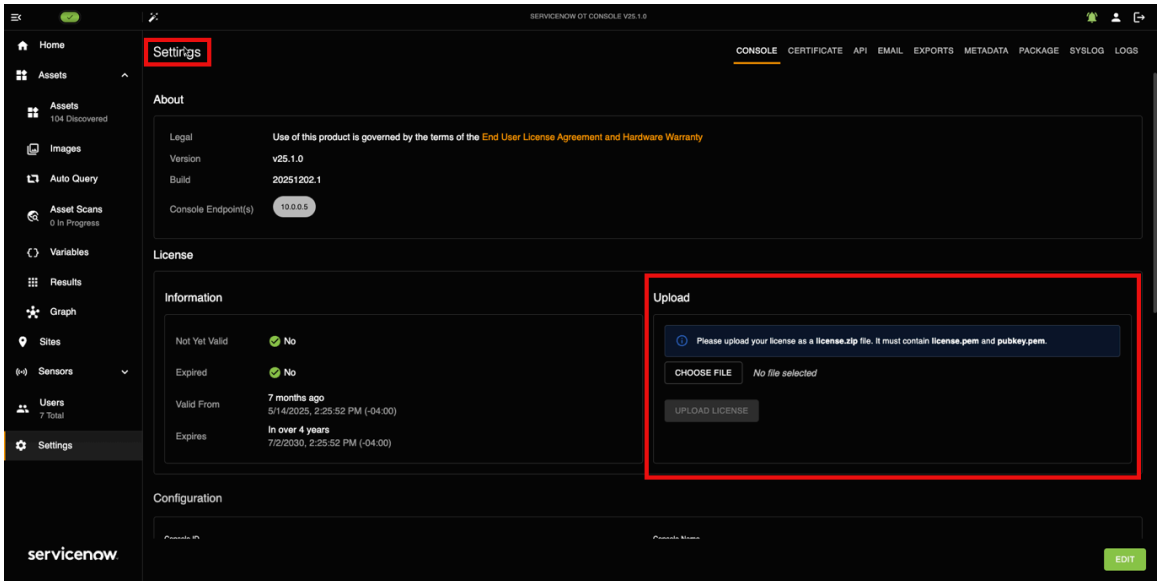
Note: Before you can use the Console, you must have a license. Request a Console license from your ServiceNow account representative.

When you first sign into the Console, a warning banner alerts you that there is no license. To upload a license for the Discovery Console for OT, do the following:

1. From the Home page, navigate to the Settings page.
2. On the Settings page in the License section, select the **Upload License** button.
3. Upload your license as a `.zip` file.
4. Verify the ZIP file contains the `license.pem` and `pubkey.pem` files.

Once you have uploaded your license, you can use the Console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Console features that require a license

It is important to understand that certain features are rendered inactive if the Discovery Console for OT license is expired. After the license expires, the locking mechanism is triggered and deactivates these features. No data is lost in the background. When a valid license is uploaded, the you can start or continue working. When the license is about to expire, the Console displays a warning banner as an alert.

The license:

- Enables the ability to run Auto Query and asset scans (inactive on expiration).
- Enables the consumption of network connection data (inactive on expiration).
- Enables the creation and viewing of API tokens (inactive on expiration).
- Enables the export of collections (for example, assets) to files (inactive on expiration).

Note: You can't export RAW XML results if your Console license is invalid (absent or expired).

Install a Linux operating system

Install a Linux operating system on a virtual machine and then install the Discovery Console for OT on the same VM.

Before you begin

Role required: admin

About this task

- Install the distribution with minimal configuration, including an SSH server, and confirm the VM supports AVX/AVX2 instructions.
- Allocate 16 GB of RAM for installation. For more information, see OT Discovery System Resources or Requirements for Discovery Console for OT installation.

Procedure

Install any of the following Linux distributions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Compatible Linux distributions

OS	Description
RedHat Enterprise Linux (RHEL) 8.x, 9x, and 10x	See https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/10#Installing%20RHEL
Rocky 8.x, 9x, and 10x	See https://docs.rockylinux.org/10/guides/installation/
Debian 12 and 13	See https://www.debian.org/releases/testing/amd64/
Ubuntu 22.04 and 24.04	See https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview

Install the Discovery Console for Operational Technology (OT)

Install the Service Graph Connector for OT Discovery before accessing the Discovery for OT packages. You must also install a Linux distribution on the same machine the Discovery Console for OT is installed on.

Before you begin

Role required: admin

About this task

Once the Linux OS is installed on the device with the Discovery Console for OT installed on it, do the following.

Note: When running the installation for any of the supported distributions, you'll want to use the minimal installation, no desktop environment, but include an SSH server in the package selection.

Important when setting up your VM environment:

- Verify that the CPU settings for the VM are set to `host`; the hypervisor/host system must include support for the AVX/AVX2 instruction set.

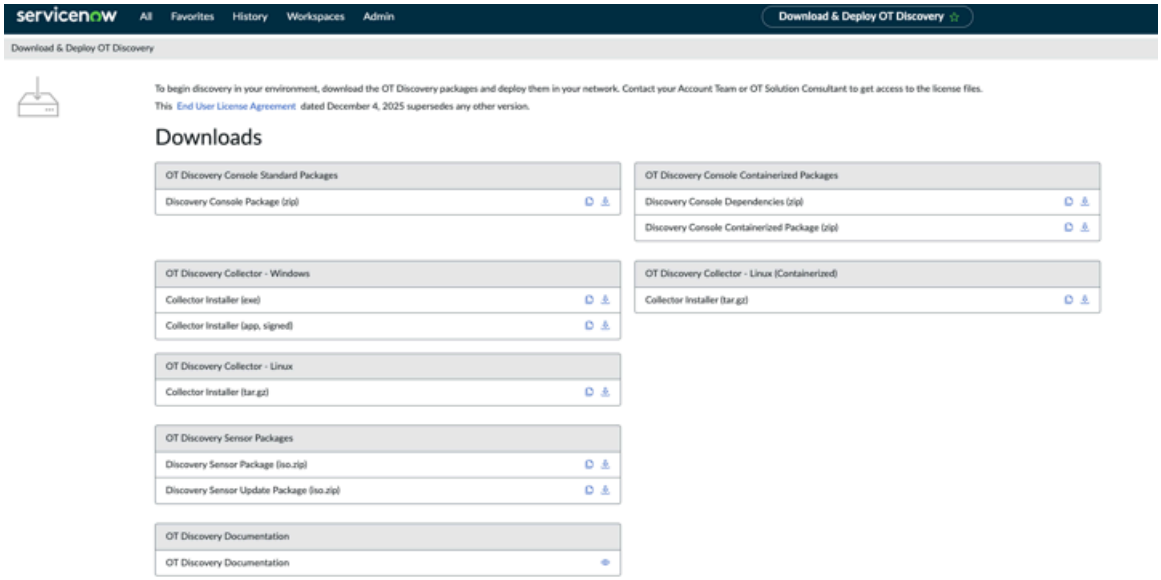
  Note: Be sure you have set this correctly; otherwise, MongoDB may crash when you attempt to restart the VM.

- Allocate 16 GB RAM for the Linux installation.
- The OT Discovery Console requires a minimum of 100 GB of storage. Increase the storage based on Deep packet capture inspection requirements. For more information, see OT Discovery deployment scenarios
- You must be on a VM to access images in the Discovery Console for OT.

Procedure

1. On your ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page.
2. Select **Get Started**.
   The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select Download & Deploy OT Discovery.
4. Select **Configure** and the **Downloads** page opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: For downloading and installing the containerized Console and Collector packages, see Air-gapped networks and OT Discovery installation.

5. On the OT Discovery page, download the Discovery packages:
   a. First download and install the Discovery Console for OT package.
   b. After the Console, download and install the Discovery Sensor for OT package.
   c. Finally, download and install the OT Discovery Collector package that is compatible with your machine's OS.

Note: Read the End User License Agreement (EULA) carefully and then check Agree.

6. From the Discovery Console for OT install package, unzip the `ConsoleInstaller` ZIP file.
7. Use the secure copy protocol (SCP) to move the ConsoleInstaller folder onto your Linux server.

   a. Push to the console:

   ```
   scp -r ConsoleInstaller serviceadmin@IP:/home/serviceadmin$
   ```

   For example:

   ```
   $ scp -r ~/Users/Zelda/Downloads/ConsoleInstaller SL
    serviceadmin@192.168.2.2:/home/serviceadmin
   ```

   Note: The ConsoleInstaller folder name can vary if so desired.

   b. Pull from the user computer:

   ```
   $ scp -r $USER@$IP:~/ConsoleInstaller /home/serviceadmin/
   ```

8. Run the console initiation script (`console.init`) via SSH.

   a. Enter the password when prompted.

   ```
   ssh serviceadmin@$IP
   ```

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. When asked if you're sure you want to continue, type `Yes`.

c. Optional: You can enter: `chmod +x console-init.sh`.

d. Then enter `sudo /bin/bash console-init.sh`.

e. Select the default answer for all prompts.

9. Verify that the web console is running.

a. Open a browser and navigate to the web console via `https://$IP:8443`.

b. When warned of a self-signed certificate error, select **Advance** and accept the EULA.

c. Create account information that conforms to your company policy and add:

- Username as the user primary admin
- Enter an email address
- Create a password (that conforms to the company policy)
- Log the username and password in a secure location
- Then select **Register**.

> **Note:** This user is the primary local admin, and it's recommended that the password is secured as well as 2FA enabled.

10. Reboot the console by entering `reboot` in the terminal window.

Result
The installation for the Discovery Console for OT is complete. Before you install the Discovery Sensor for OT package, install the Discovery Console for OT certificate. For more information, see Generate a certificate.

> **Note:** If you encounter any errors, Contact Customer Service and Support.

Log on to the Discovery Console for OT

This sections describes your initial log onto the OT Discovery Collector.

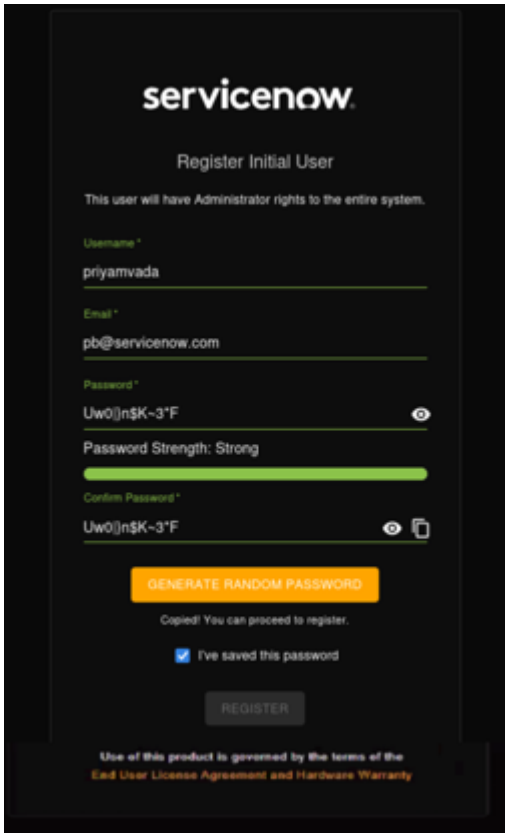
Initial log in to the Console

After installing the Discovery Console for OT you're initially prompted to register and log in to the Console. This initial login gives you administrative rights throughout the entire system.

You're prompted to fill in your username, email, and password. The window indicates the strength of your password. You can select **Generate Random Password** instead of creating a password.

Copy or note the password you entered or generated. Select the check box next to **I acknowledge I saved this password**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Generate a certificate

Generate a certificate to use with the Discovery Console for OT or upload your own certificates. This certificate allows the Console to boot up.

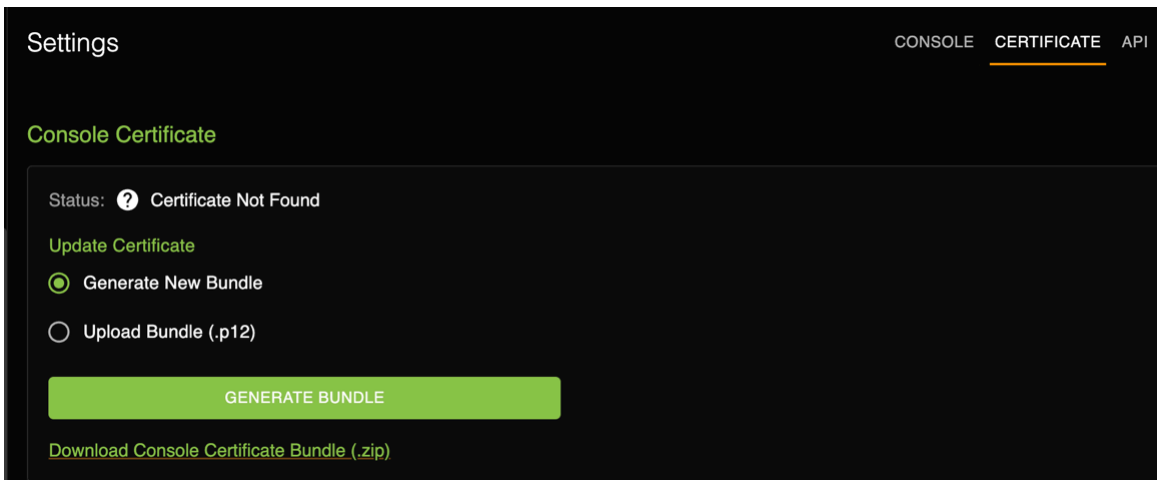
Before you begin

Note: If you choose to do so, you can create your own certificate if it is required by your company's policies.

Role required: admin

About this task

After the Discovery Console for OT is installed, there are default, preloaded certificates that power up the Console. However, following this initial boot, it's recommended that you use the Console to generate a new Certificate Authority (CA). This task describes your options for generating the Console CA.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You can also select the link **Download Console Certificate Bundle (.zip)**. For more information, see the table.

Procedure

1. Navigate to the Discovery Console for OT **Settings > Certificate** tab.
2. Generate a new bundle, upload an existing bundle.

Note: You're not obligated to use the ServiceNow provided certificates and you may choose to use your own.

Option	Description
Generate a new bundle	**a.** Under **Update Certificate**, select **Generate New Bundle**. **b.** Select the **Generate Bundle** button.
Upload an existing bundle	**a.** Under **Update Certificate**, select **Upload Bundle (.p12)**. **b.** Use the **Choose File** button and select the bundle to upload. **c.** Enter a **Bundle Password**. **d.** Select the **Upload Bundle** button.
Download Console Certificate Bundle (.zip)	The bundle contains the Console's Certificate and the web browser certificate. These certifi cates establish trust between these applica tions and confirm their communications are secure and encrypted.

Note: Generating or uploading a certificate also updates any current certificates.

Result
A certificate is generated. The Discovery Console for OT reboots.

Upgrade the Discovery Console for OT

These are the instructions for upgrading the Discovery Console for OT. The scope of this document does not include how to upgrade the containerized version of the Console.

Before you begin
You must have the latest version of the Console already been installed on one of the supported Linux distributions.

Note: After the March 2026 GA release of the Console, the version of the .Net runtime has been changed from 8.x to 10.x since the 8.x version has an End of Support date of November 10, 2026.

The Console packages now require .Net 10.x. The console-upgrade.sh script included with `consoleinstaller` builds of 20260527.3 or later attempts to install this dependency before making any other changes to the system. This requires internet connectivity for the upgrade installation. If the script determines .Net 10 is not present on the system and is unable to install it, it exits before attempting to upgrade to the new set of Console packages.

Also, Rabbit 4.3 was released after the GA release. This script does not attempt to make any changes to accommodate a newer Rabbit version, because:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- the system is still running the version installed at the time of the original Console installation, **OR**,
- if Rabbit was upgraded after that, this was intentionally done by the end user, and this end user has already updated the Rabbit version.

Role required: admin

Procedure

1. Transfer the new `consoleinstaller` package over to the system hosting the Console.
2. Unzip the package by typing `unzip [name of console installer package]`.

   Note: If you run this command in a directory where there is already a ConsoleInstaller folder present, you're prompted with: `replace ConsoleInstaller/docs/codeowners.md? [y]es, [n]o, [A]ll, [N]o, [r]ename:` Type A followed by Enter/Return to continue unzipping the files.

3. Change directory to the ConsoleInstaller folder by typing `cd ConsoleInstaller`.
4. Type `chmod +x console-upgrade.sh` to make sure the upgrade script is set to be executable.
5. The Console upgrade script needs to run with root privileges.

   Include desired level of detail for using either `su` or `sudo` to do that.

6. Run the upgrade script by typing the following command: `/bin/bash console-upgrade.sh`.
   Depending on the current state of the system, you may be prompted with a few questions to complete the upgrade process. The console upgrade script can run the latest migration scripts automatically with no user input needed. This requires Console installer program version 20260601.8 or later for `devslim`.

Use the Discovery Console for OT pages

Get started with the Discovery Console for OT application after it is installed and configured.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Navigating the Console pages

The Discovery Console for OT is organized into multiple pages navigated by the side navigation panel. Each page displays specific tasks you can accomplish. Every page contains information and step-by-step procedures for using the Discovery Console for OT to query and inventory in your OT environment.

The next sections describe the Discovery Console for OT pages and how to use the Console's features.

Home page

The Home page on the Discovery Console for OT provides a dashboard overview of the assets and sites on your current system.

In the navigation menu, you can select the Assets and Sensors pages to reveal sub-menus. You can select Sites, Users, and the Settings items for more data.

The Console opens to the Home page.



The **Home** page is made up of a left-hand, expandable navigation menu and a main area; that is, the Assets Dashboard. The dashboard is divided into the following sections.

- Assets section
- Assets by Location section
- KPI cards section

Assets

The Assets section gives you an overview of the assets and sites available in your system, organized by widgets. The widgets are the following:

- **All**: List of all the assets in your system.
- **New**: List of the most recently discovered assets.
- **Modified**: List of the most recently edited or updated assets.
- **Sites**: List of all current sites.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

By selecting the **All** widget, you can view the list of all the assets in your system. The **New** widget takes you to a list of the most recently discovered assets. The **Modified** widget takes you to a list of the most recently edited or updated assets. The **Sites** widget lists all current sites available in the Console.

Underneath these widgets are two graphs: **New Assets** and **Modified Assets**. The graphs display asset information organized by date.

Under these graphs are the **By Brand** and **By Port** graphs. The **By Brand** graph breaks up your assets according to brand. The **By Port** graph breaks up your assets based on the available ports that they're connected to. Selecting a section on either of these images takes you to the asset list filtered by the selected brand or port.

The following image shows an example of the data that you can find in the Assets section.

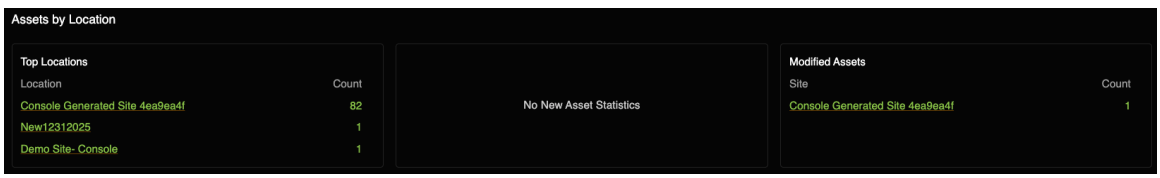


Assets by Location

The Assets by Location section provides the number of assets according to the available site. The location of an asset is dependent on the Site's IP ranges that you define when creating a site. For more information about creating a site, see Add a Site.

The **Top Locations** widget ranks each location based on its number of assets. The **New Assets** widget calls out any recently discovered assets by Site. The **Modified Assets** widget calls out recently edited or updated assets by site.

The following image shows an example of the data that you can find on the Assets by Locations section.



Keyswitch / Protection

The Keyswitch / Protection section displays any key switch security or protection that you can have for your system assets. The following image shows an example of the data that you can find in the KeySwitch / Protection section.

Note: The Keyswitch / Protection section is only available if you have data available in your system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



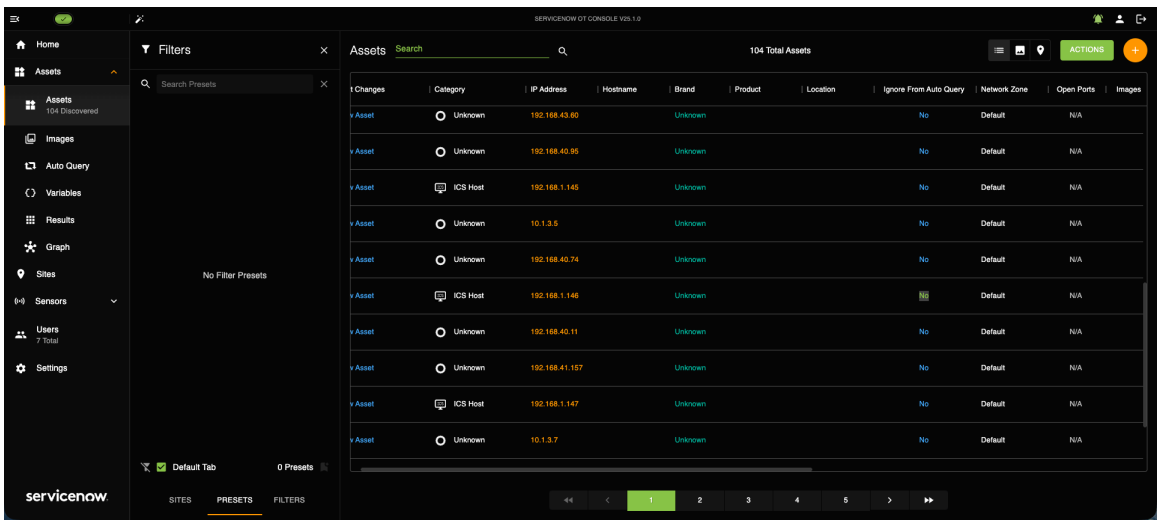
Assets page

The Assets page shows a list of all available assets for the Discovery Console for OT.

Note: To edit any of the fields in the Asset record, select the asset from the list and then select the Edit button. After editing, select Save to save any changes.

Assets page overview

The Assets page shows all assets that were automatically discovered along with all assets that were manually added to the system. To view the assets list, use the navigational menu on the left side of the screen and select **Assets > Assets**.



You can add assets with the following methods.

- Sensors and Collectors perform Native discovery and populate the assets.
- Import via a CSV with assets information.
- By selecting the add icon .

Filter panel

When you open the Assets page, there is a Filter panel you can use to filter which Assets appear in the list. There are preset filters which appear as tabs at the bottom of the panel. The preset filters are (you can also check the Default Tab box):

- Sites
- Presets
- Filters

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select the X at the top of the panel to close the filter. To open the panel, select the filter icon .

Views

In the top right area of the Assets list, there are different icons that control how the Assets are viewed.



The views are:

- List view
- Gallery view
- Map view

Actions

The **Actions** button provides a drop-down menu for manipulating the Assets. The formats for each are indicated next to the selection where applicable. The selectable actions are:

- Import Assets
- Import Ignore Assets (CSV)
- Export Ignore Assets (CSV)
- Export Assets (JSON)
- Export Assets (CSV)
- Update Manufacturer Data
- Update Vulnerability Data
- Update Product Mappings
- Update Purdue Levels
- Ignore Assets
- Delete Assets

Note: If an action is inactive, it appears grayed out in the menu.

Next to the **Actions** button is the add icon .

Asset records

With an Asset record, you can view and edit the details of the selected asset. To view an asset record from the Assets page, select the IP address displayed for the asset. The following sections describe each section of an Asset record.

Note: When you select the add icon , this same view opens with these same sections. However, when you open an existing asset record, you have three tabs on the upper right side of the screen. The tabs are **Details**, **Images**, and **Modules**.

Identification

The Identification section contains the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
IP Address [Required]	IP Address assigned to the asset.
Hostname	Name of the connected device. **Note:** The name is populated when it is configured on the device or if the DNS server is configured.
Product	Manufacturer and model of the asset.
Firmware Version	Version of the firmware installed.
Network Zone	Network zone of the asset.
MAC Address	MAC address that is associated with a given asset.
Serial Number	Serial number associated to the asset.
Ignore from Auto Query	Option to mark devices that must be ignored from the auto queries. This field is automatically set to inactive,

Classification

The Classification section contains the following fields.

Field	Description
Auto Categorization	Feature that enables the Discovery Console for OT to manage and update the **Description**, **Category**, and **Operating System** fields through the automatic classification system. Set to Yes or No. **Note:** If **Auto Categorization** has been enabled, then editing is turned off for the **Category**, **Brand**, **Operating System**, and **Details** fields. Users can select Edit and then modify the values during editing. To delete an asset, set **Auto Categorization** to **No**. The **Delete** button then appears in the right-most column allowing you to delete the asset.
Category	Category or classification indicates the function of the device or class that the asset belongs to. For example, Desktop, HMI, PLC, or SCADA.
Brand	Name of the manufacturer that produced the asset.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Purdue Level	N/A by default. See image of drop-down choices.
Operating System	Operating system of the asset. For example, IOS, Linux, or Windows.
Details	Section for additional details to describe the classification for this asset.

Timeline

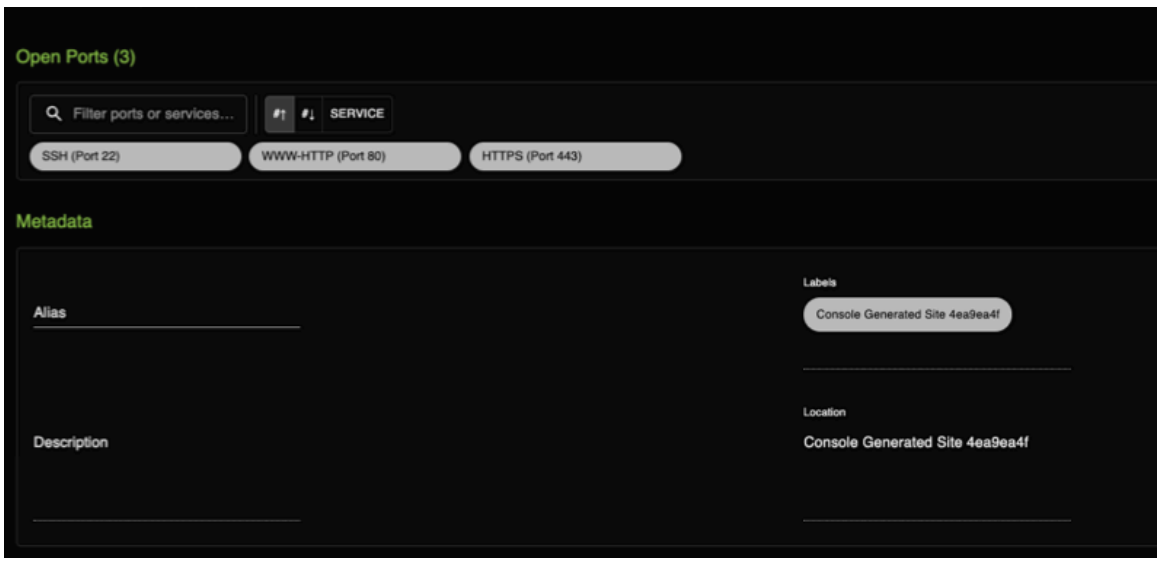
The Timeline section contains the following dates and times related to the asset.

Timeline

Field	Description
Created	When the asset was created.
Modified	The last time the asset was modified.
Last Seen	The last time the asset was detected.
Updated	The last time the asset was updated.

Open Ports

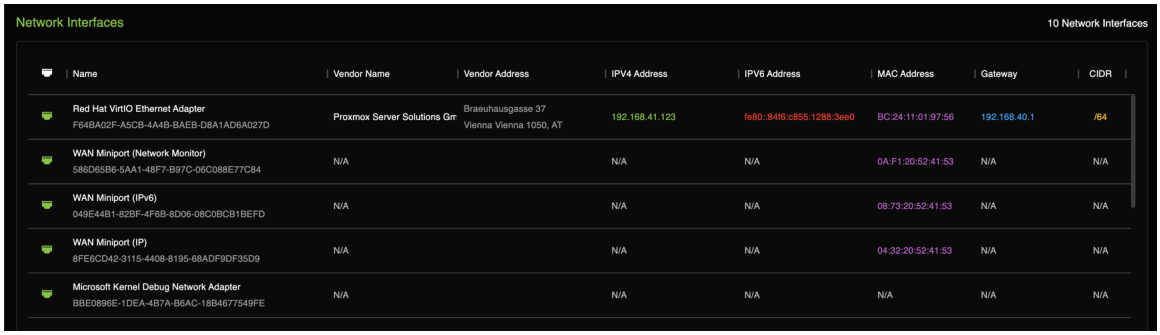
The Open Ports section lists all open ports available on the asset that were identified by Discovery and shown on the Discovery Console for OT.



Network Interfaces

The Network Interfaces section displays the Asset's Vendor, Vendor Address, IPV4 Address, IPV6 Address, MAC Address, Gateway, and CIDR.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Metadata

The Metadata section contains the following fields.

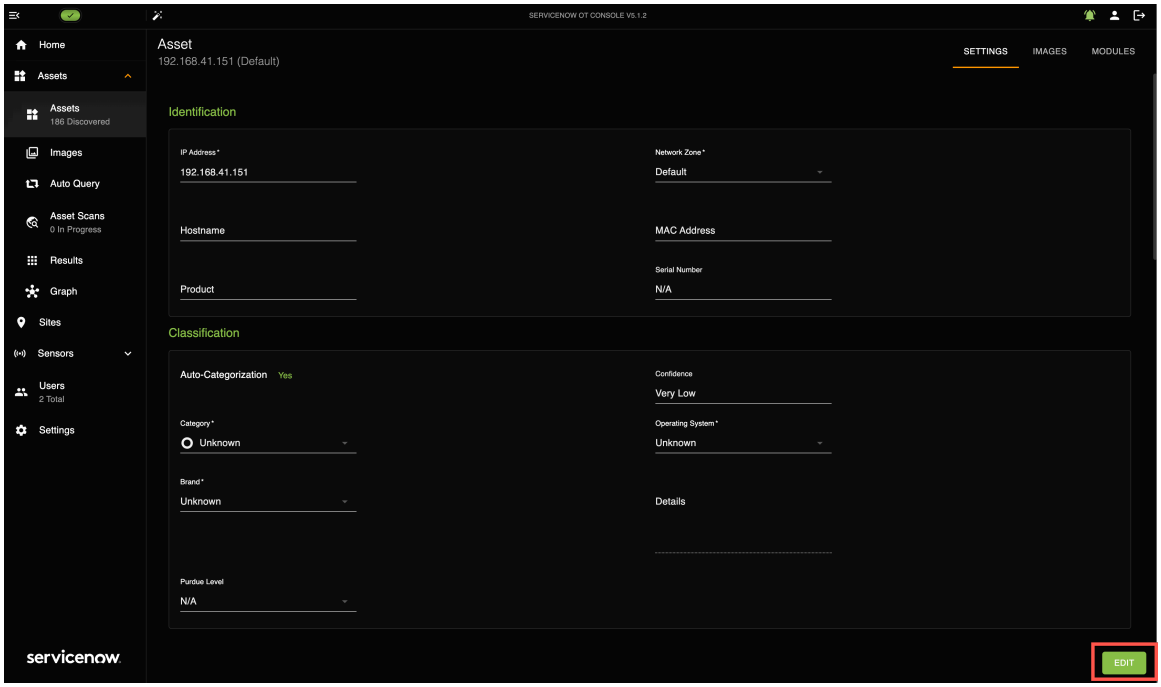
Field	Description
Alias	Alternate name given to the asset. Where possible, the alias is displayed instead of the IP Address or MAC address to provide a user-friendly way to identify the asset.
Description	Description of the asset.
Labels	Tag that you can add to an asset to assist in identifying and finding assets with the tagged properties within the system.
Location	Description of the physical location of the asset.

Installed software

The Installed Software section includes a list of all software installed on the asset. To add software, complete the following actions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Select the **Edit** button.



2. Scroll to the Installed Software section and select **Add Software**.



3. In the Add Software modal window, enter the **Vendor**, **Product**, and **Version** (optional) of the software being added.
4. Select **Save**.

The added software displays in the Installed Software list.

Attributes

The Attributes section contains the attributes discovered by the Discovery process. To add an attribute, complete the following actions.

1. Select the **Edit** button.
2. Scroll to the Attributes section and select **Add Attribute**.

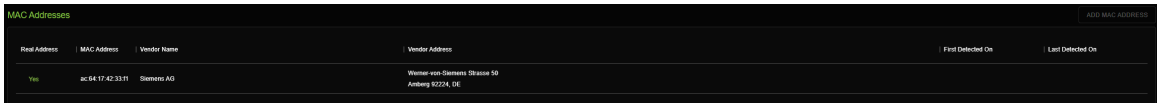


3. In the Attribute modal window, enter the **Name** and **Value** of the attribute.
4. Select **Add Attribute**.
5. Select **Save**.

MAC Addresses

The detected MAC Addresses section includes a list of all the MAC addresses that are associated with a given asset. The Real Address toggle is used to indicate that a MAC address belongs to an asset and should be considered the primary or main MAC address. Each detected MAC address in the list includes the **Vendor Name**, **Vendor Address**, **First Detected On**, and **Last Detected On** fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



To add a MAC address, complete the following actions.

1. Select the **Edit** button.
2. Scroll down to the MAC Addresses section and select **Add MAC Address**.
3. In the Add MAC Address modal window, add the name of the MAC Address.
4. Select **Add Mac Address**.
5. Select **Save**.

Comments

The Comments section provides an area to enter additional information about the assets. To add a Comment, complete the following actions.

1. Select the **Edit** button.
2. Scroll to the Comments section and select **Add Comment**.



3. In the Add Comment modal window, enter a comment.
4. Select **Save**.

The added comment is listed in the Comments section of the asset.

Create an asset

Manually create an asset to the Discovery Console for OT.

Before you begin

Role required: admin

Procedure

1. Navigate to the **Assets** page.
2. Select the add icon.
3. In the **Create Asset** page, fill in the following sections.
   - **Identification**: If applicable, add the following information:
     - **IP Address**: Required.
     - Hostname
     - Product
     - Firmware Version
     - Network Zone
     - MAC Address
     - Serial Number
     - **Ignore from Auto Query**: Slide toggle to set to Ignore.
   - **Classification**: If applicable, add the following information:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Category**: Required. Provides a pop-up list to choose from.
- **Brand**: Required. Provides a pop-up list to choose from.
- **Purdue Level**: Optional. Provides a pop-up list to choose from.
- **Operating System**: Required. Provides a pop-up list to choose from.
- **Details**: Optional.

- **Network Interfaces**: Displays available network interfaces.
- **Metadata**: If applicable, add the following information:
  - Alias
  - Description
  - Labels
  - Location
- **Installed Software**: If applicable, select the Add Software button and select the software you want to include.
- **Attributes**: If applicable, select the Add Attribute button and select the Attributes you want to include.
- **MAC Address**
- **Comments**: If applicable, add comments.

4. Select **Create Asset** to create an asset or select **Cancel** to discard your entries.

Result
The asset is created and added to the Assets page.

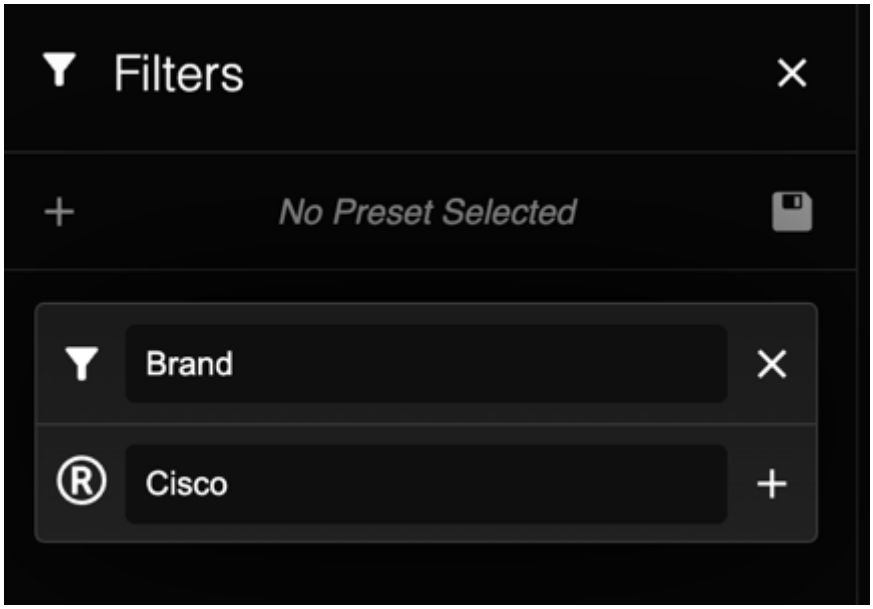
Deleting assets in bulk

Filter assets and do a bulk deletion in the Discovery Console for OT.

Before you begin
Role required: admin

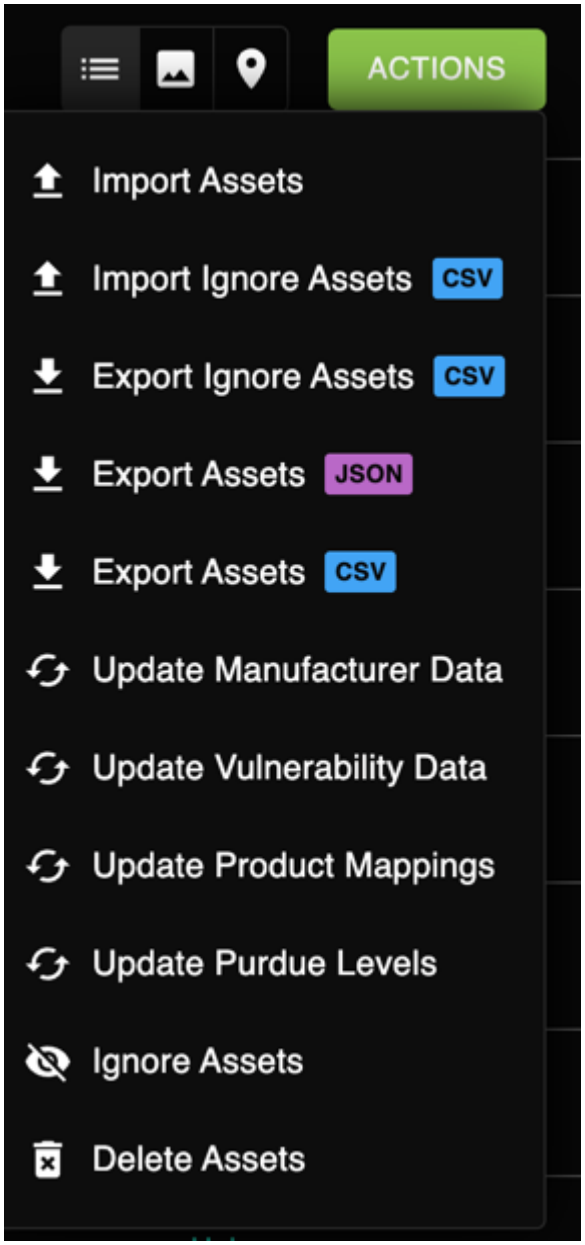
Procedure
1. Navigate to the Assets page.
2. In the Filters pane, select the bottom tab, **Filters**.
3. Select the plus sign at the top of the pane.
4. In the new entry field, select a filter type from the pop-up menu by selecting the down arrow icon  .
   For example, if you select Brand, a second entry field options and provides a pop-up list of brands. You can select more than one type of filter and the associated list, but you can only delete one group of assets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



5. After you have filtered your assets, select **Enter**.
   The selected assets are set in the filter pane.
6. Select the **Action** button.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



7. Select **Delete Assets**.
   You're prompted to confirm deleting assets.

Result
The bulk deleted assets are no longer in the Assets table.

Import or export assets

You can import or export assets, and ignored assets, to either CSV or JSON formats.

Before you begin
Role required: admin

Procedure

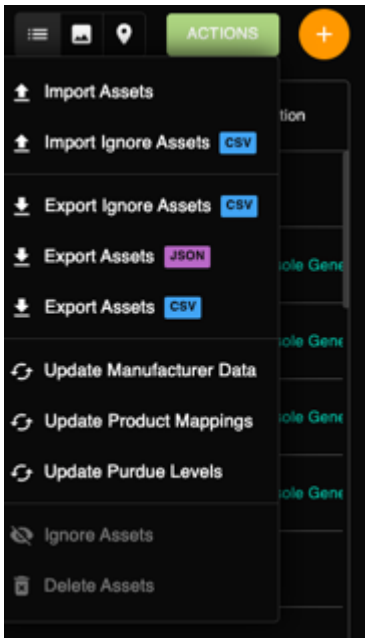
1. Navigate to **Assets > Assets** page.
   The list of current assets displays on the page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

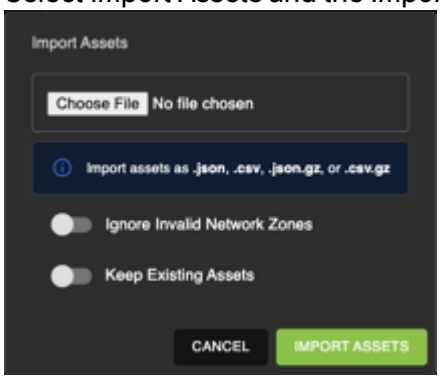
2. You can import/export all listed assets or you can filter the list using the Filter panel, selecting the Filter tab.
   For more information, see Assets page.

Import assets

3. Select the**Actions** button.



4. Select Import Assets and the Import Assets window opens.

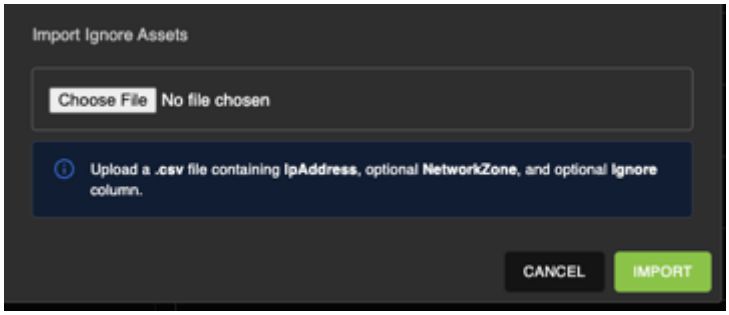


   The window lists the format you can import to the Console. You can also toggle the available settings in the window to activate them:

   - Ignore Invalid Network Zones
   - Keep Existing Assets

5. When you select Import Ignore Assets, the prompt window opens and displays the additional required information needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

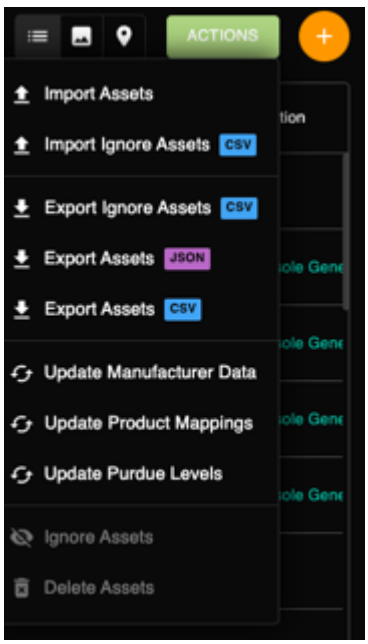


Note: The assets file must be in CSV format to upload to the Console.

6. Other actions and formats you can select from the **Actions** menu are:
   - Export Ignore Assets (CSV)
   - Export Assets (JSON)
   - Export Assets (CSV)

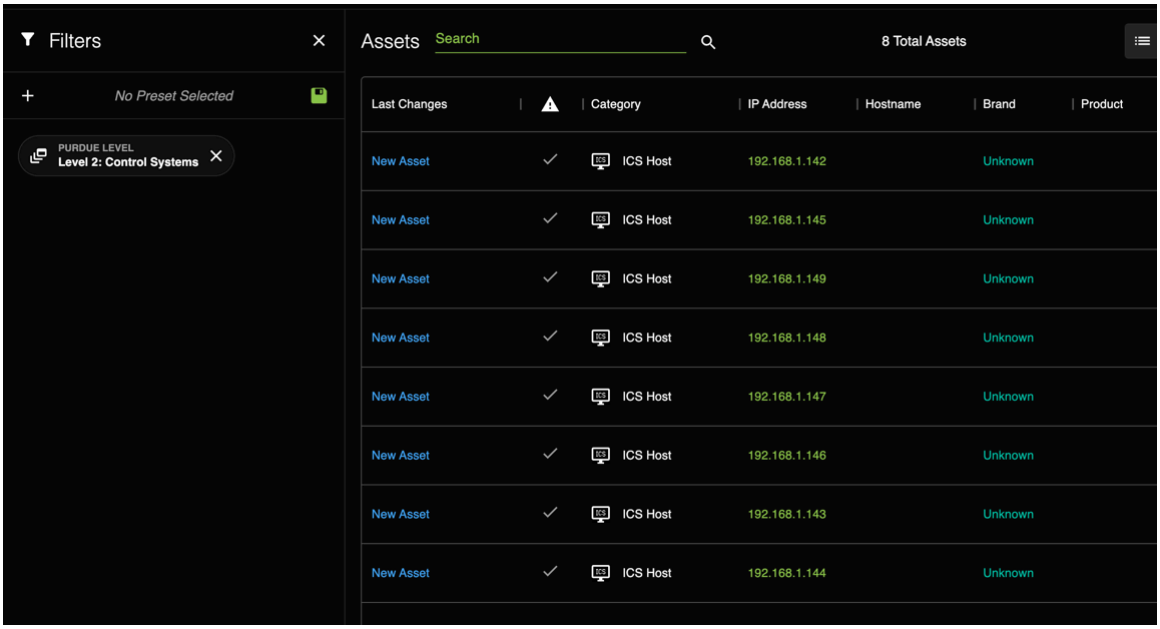
Export assets

7. Select the**Actions** button.



8. Select Export Assets by the format you want the output to be.
   Choose to export either .csv or json asset files. If you don't choose a specific asset or assets, all asset information is exported.
9. Use the Filters panel to sort the assets you want to export.
   In this image, the assets are filtered by the general type Purdue level and the more specific Level 2.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



10. From the Actions menu, select Export Assets for the desired format, either .json or .csv. The filtered assets are exported.

Images page

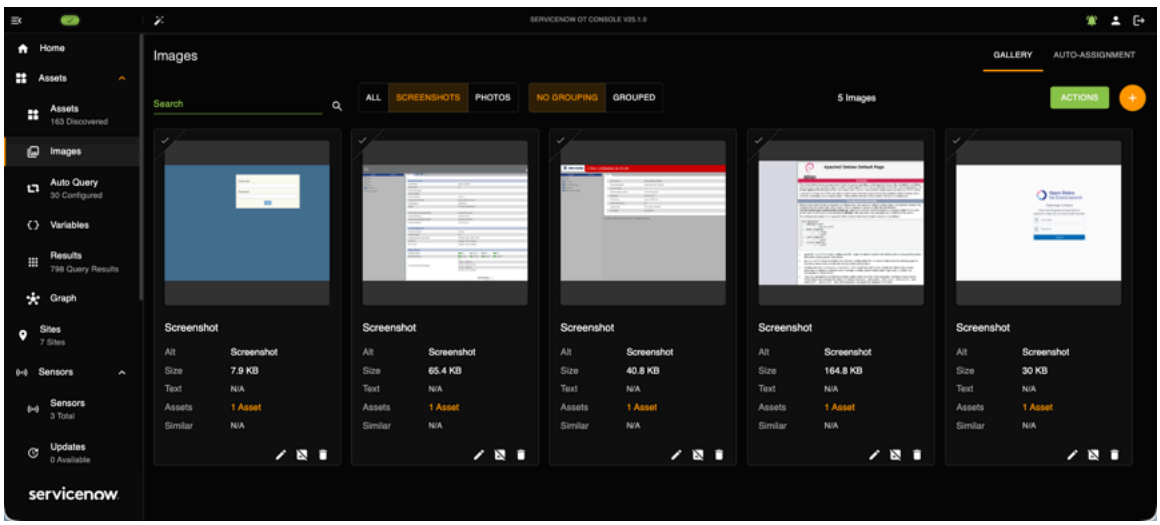
The Images page contains the images related to your Discovery Console for OT assets.

On the Images page, you can view, add, and manage photos and screenshots captured during the Discovery process related to your assets on the Console.

Note: When you import any assets, image data aren't imported.

The Images page allows you to search for an image. The page has the following tabs:

- **Gallery** tab: Displays images.
- **Auto-Assignment** tab:



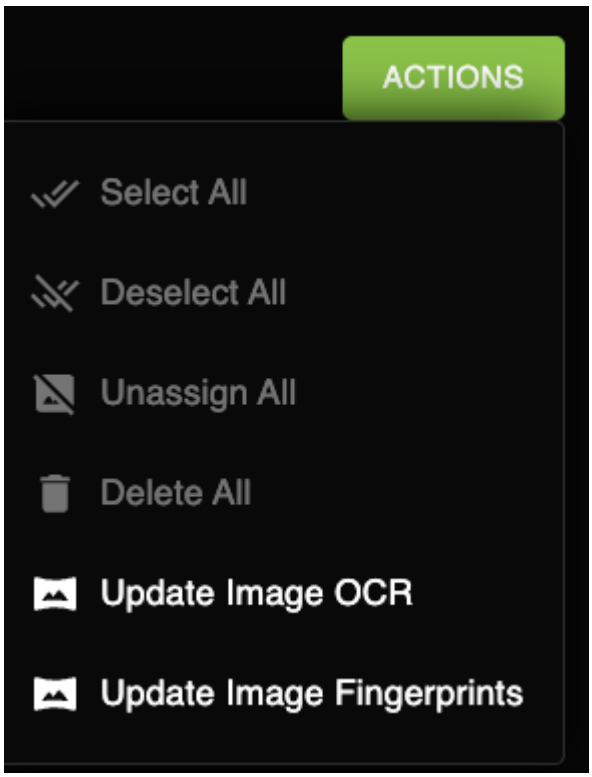
Gallery tab

The Gallery tab shows different views of the images:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- All: View all images.
- Screenshots: View only screenshot images
- Photos: View only photo images
- No Grouping
- Grouping

On the Gallery tab, select the **Actions** button and select from the drop-down menu.



Select the add icon to browse and upload images. You can also just drag and drop the image on the window.

Auto-assignment tab

Under the **Auto-Assignment** tab, you can select the add icon and open the **Edit Auto-Assignment Profile**.

To add an image, select the add icon.

To delete an image, select the delete icon.

Note: To capture screenshots during the Operational Technology Discovery process, the Full Web Extractor Auto Query needs to be selected and executed. This captures the screenshots over ports 443 and 80 and extracts the content from the web pages.

Auto Query page

The Auto Query page contains the automatic asset queries for the Discovery Console for OT.

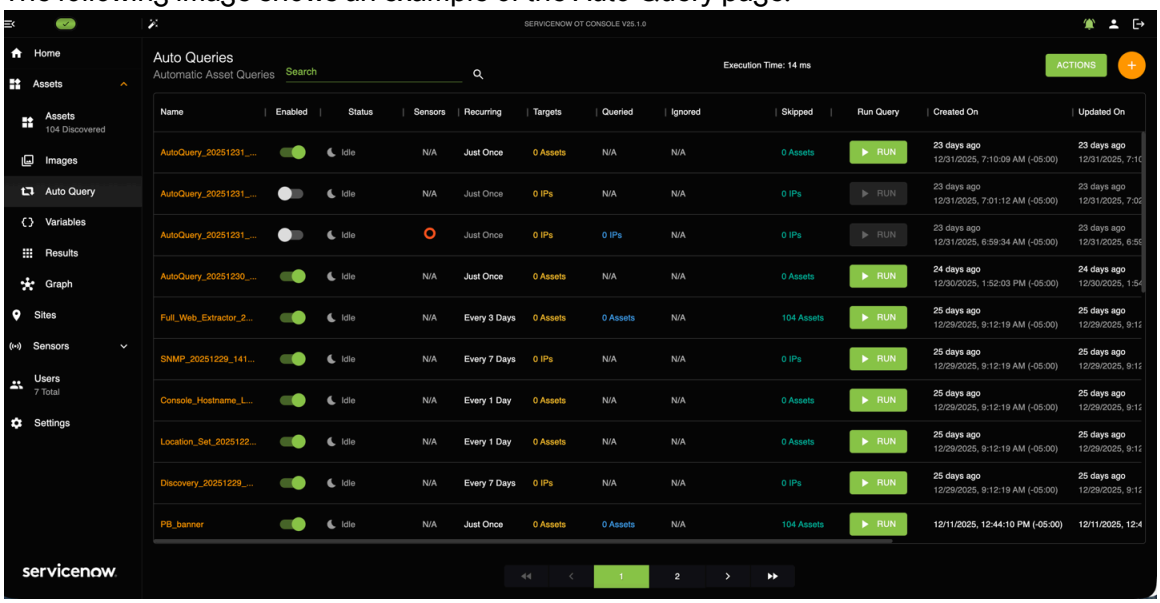
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Auto Query

The Auto Query page contains a list of all the automatic asset queries available for your system. Each Auto Query is displayed in columns with the following headings and information.

- Name
- Enabled
- Status
- Sensors
- Recurring
- Targets
- Queried
- Ignored
- Skipped
- Run Query
- Created On
- Updated On
- Last Executed On
- Completed
- Delete

The following image shows an example of the Auto Query page.

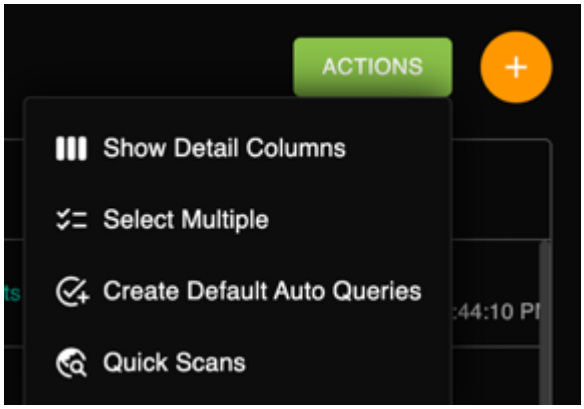


Note: When a query is enabled but not running, the Status column displays idle icon 

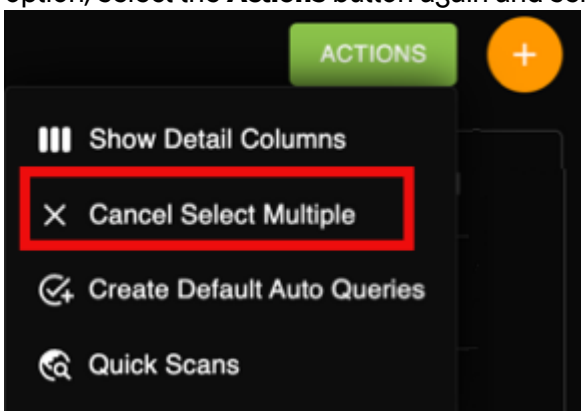
to indicate it is idle. When related or all Sensors are offline, the All Sensors Offline icon  displays.

Use the drop-down **Actions** button to select additional options.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- **Show Detail Columns**: Toggles between Show and Hide. When showing the Detail Columns, additional columns display on the page. The additional columns shown include:
  - Run Count
  - Last Run Started
  - Last Run Ended
  - Next Scheduled Run
  - Current Sites
  - Last Delay
  - Exec Time
- **Select Multiple**: Opens check boxes by each query in the list. You can check a box and the **Delete Selected** option is activated. This option deletes the selected queries. To turn off this option, select the **Actions** button again and select **Cancel Select Multiple**.



- **Create Default Auto Queries**: There are 5 default queries to choose from. Selecting this option opens the Create Auto Queries window. Select from the following default auto queries:
  - **Console Hostname Lookup**: Reverses the DNS look up performed by Console.
  - **Asset ICS Discovery**: Finds the ICS assets based on common open ports and queries using native protocols.
  - **Location Set**: Sets a label and a location field using the Site name.
  - **SNMP**: Queries to discover SNMP service. This tries only the SNMP port.
  - **OS Detection**: Use with caution, especially in production environments. This query can disrupt or crash poorly configured or sensitive assets. Queries Linux / Windows endpoint for any discoverable services.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Quick Scans**: When selected, this selection displays a list of any current Quick Scans. You can create a Quick Scan by selecting the add icon . Set the parameters of the Quick Scan in the Create Quick Scan page. Quick Scans are meant to run quickly and only once. Quick Scan targets can be assets selected by their URLs, IP Addresses, or IP ranges. For more information on Quick Scans, see Create a Quick Scan.

Create an Auto Query

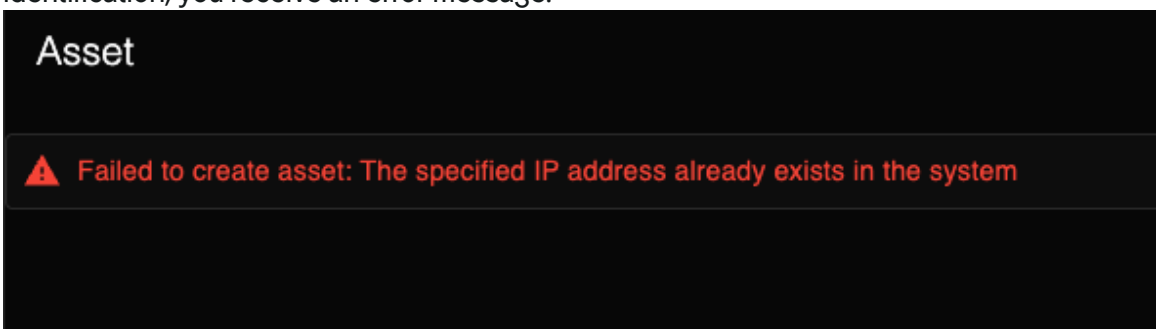
Create an Auto Query that you can run on demand for different Discovery Console for OT Assets.

Before you begin
Role required: admin

Procedure

1. Navigate to **Assets > Auto Query**.
2. Select the add icon .
3. For the Identification section, use the automatically provided name or create your own name.

   Note: If you use an IP address that is already in the system as the new Asset identification, you receive an error message.

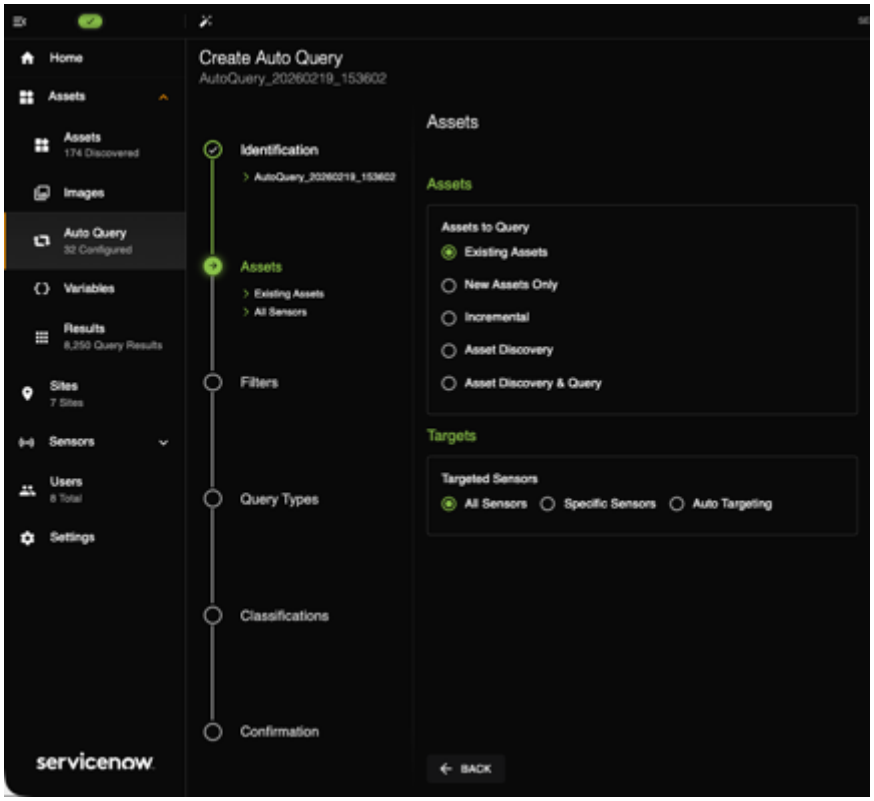
   

   Be sure to use an IP address that is not in the system already.
4. Select **Next**.
5. In the Assets section, choose from Assets and Targets.
   The available **Assets** are:
   - Existing Assets
   - New Assets Only
   - Incremental
   - Asset Discovery
   - Asset Discovery & Query

   The default Asset selection is **Existing Assets**.

   When **Existing Assets** is selected for a query, the query uses the asset's IP address and Network Zone as its unique identifier. This allows the asset's IP address to exist across multiple Network Zones.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Targets refers to Sensors and Collector.
   The available **Targets** are:
   - All Sensors
   - Specific Sensors
   - Auto Targeting

   The default Targets selection is **All Sensors**. **All Sensors** uses all available Sensors and Collectors for the query. **Specific Sensors** uses only the selected Sensor and Collectors for the query. **Auto Targeting** tries to intelligently assign targets to Sensors and Collectors based on the query. It helps manage complex deployments.
7. Select **Next**
8. In the Filters section, select the filters as needed.
   These filters help with the query selections. Filters include the following categories.

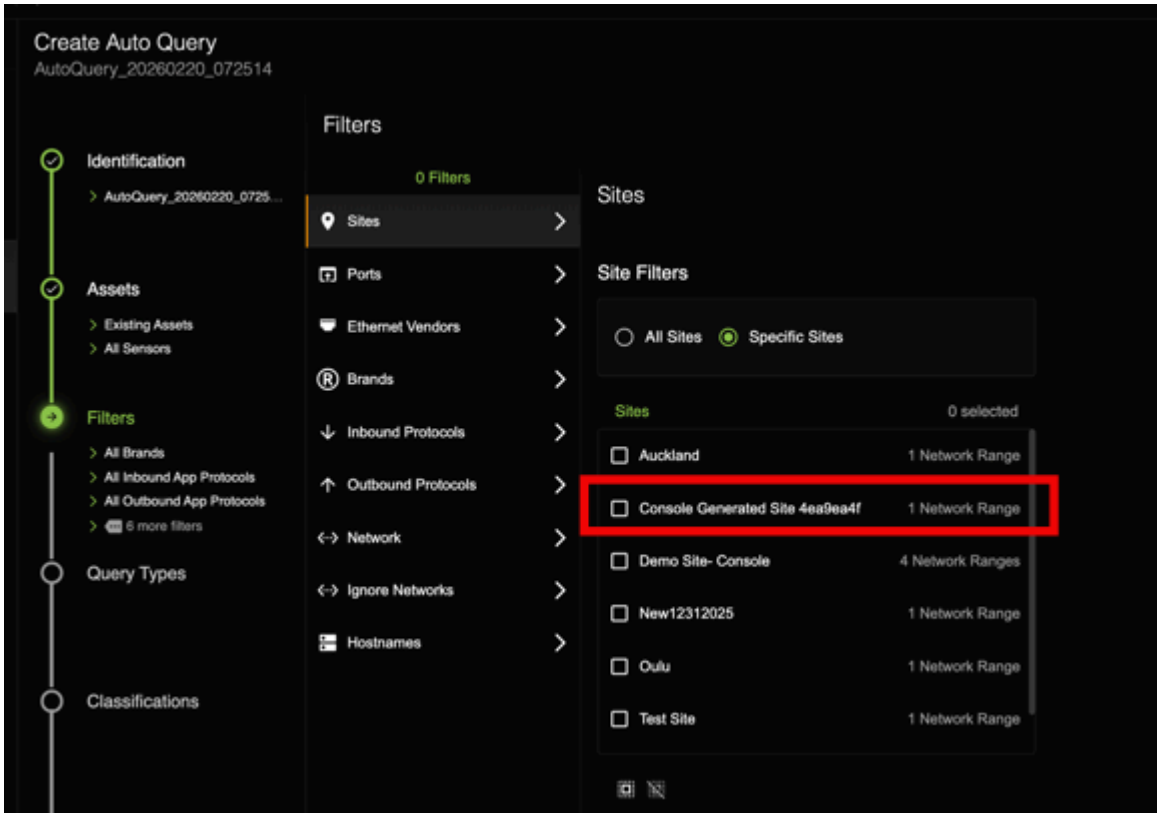
   Note: Some options in this section are only visible when the Assets selection is set to Existing Assets or Incremental. When the selection is Asset Discovery or Asset Discovery & Query, a few options are inactive.

   - **Sites**

     Site rules override global behavior when the Site filter is selected. If no site rules matches the Asset, the query skips the Asset.

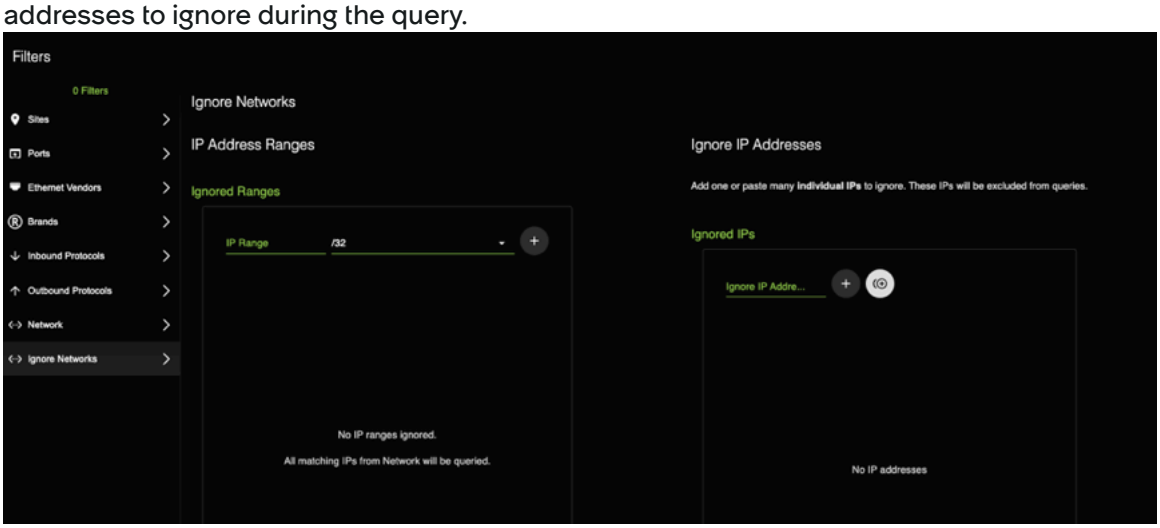
     Note: The Console automatically generates a default site. This is in case no Sites have been previously created. You can select the Console-generated site when using the Sites filter to select specific sites.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- Ports
- Ethernet Vendors
- Brands
- Inbound Protocols
- Outbound Protocols
- Network
- Ignore Networks

Note: The Ignore Networks filter allows you to select an IP range or individual IP addresses to ignore during the query.

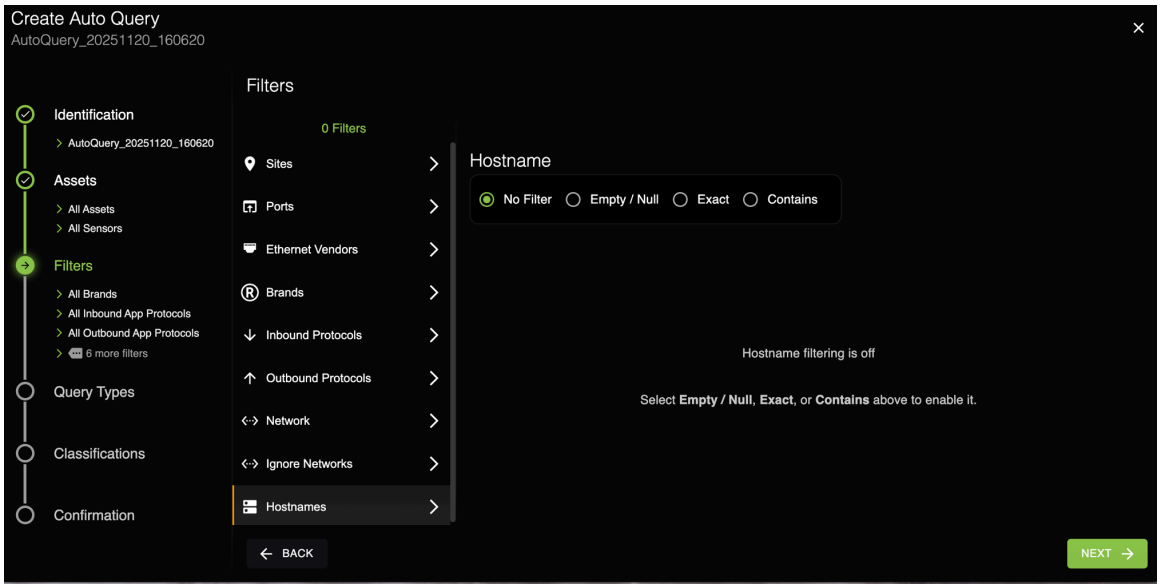


- Hostnames

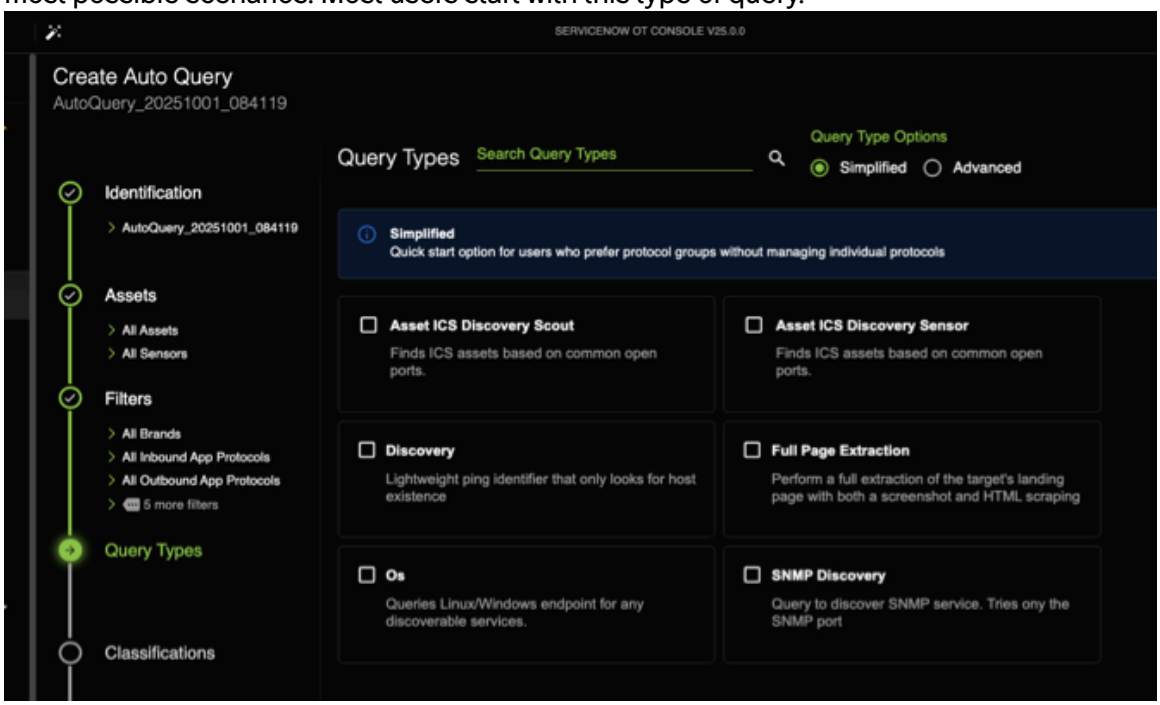
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Hostnames filter uses the hostname of the Asset and Targets the Asset based on the specified hostname information. To use this filter, select **No Filter** (default selection) or one of these options:

- **Empty/Null**: Queries Assets where the Hostname field is empty or null.
- **Exact**: Matches Assets whose Hostname equals any of the values you add. There is a field to type in a Hostname. All hostnames are included in this query unless you add at least one value.
- **Contains**: Matches Assets whose Hostname contains any of the substrings you add. There is a field for adding a value. All hostnames are included in this query unless you add at least one value.



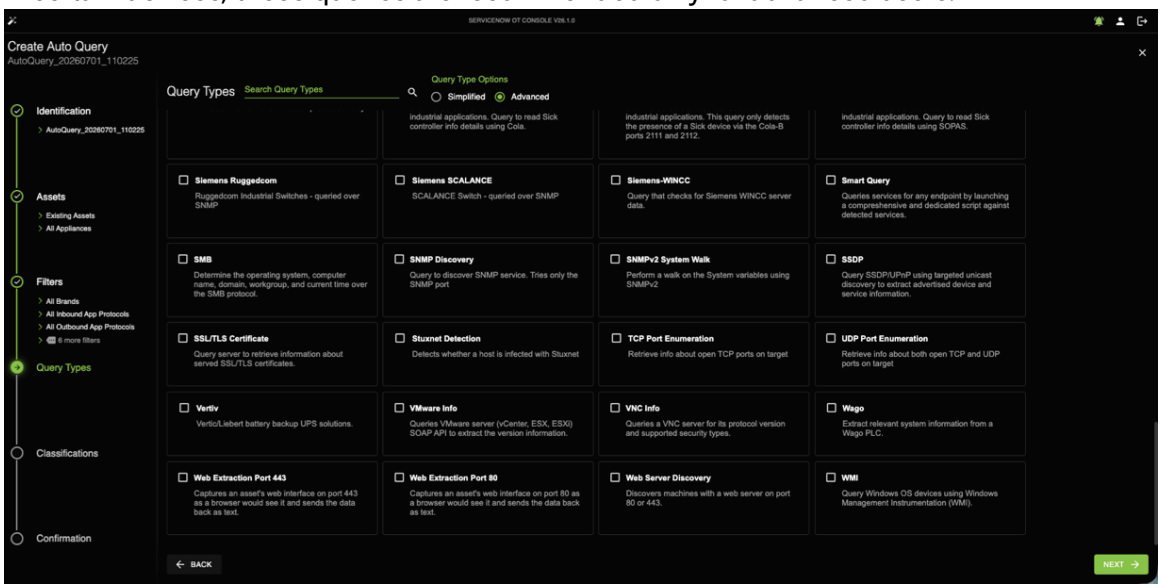
9. Choose a filter and then select **Next**.
10. In the Query Types section, select the applicable query types as needed.
    - The Simplified query types are a small list of easy-to-understand queries that should cover most possible scenarios. Most users start with this type of query.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

> **Note:** The simplified **Auto Query** type **Full Page Extraction** updates the query to perform a full extraction of your Target landing page. That means, this type of query includes both the screenshot and the HTML information.

- The Advanced query types are a list of all available advanced auto queries. As some of these queries can be riskier, require more technically complicated to understand, or specific to certain devices; these queries are recommended only for advanced users.



Some recently added Advanced Query types include but aren't limited to:

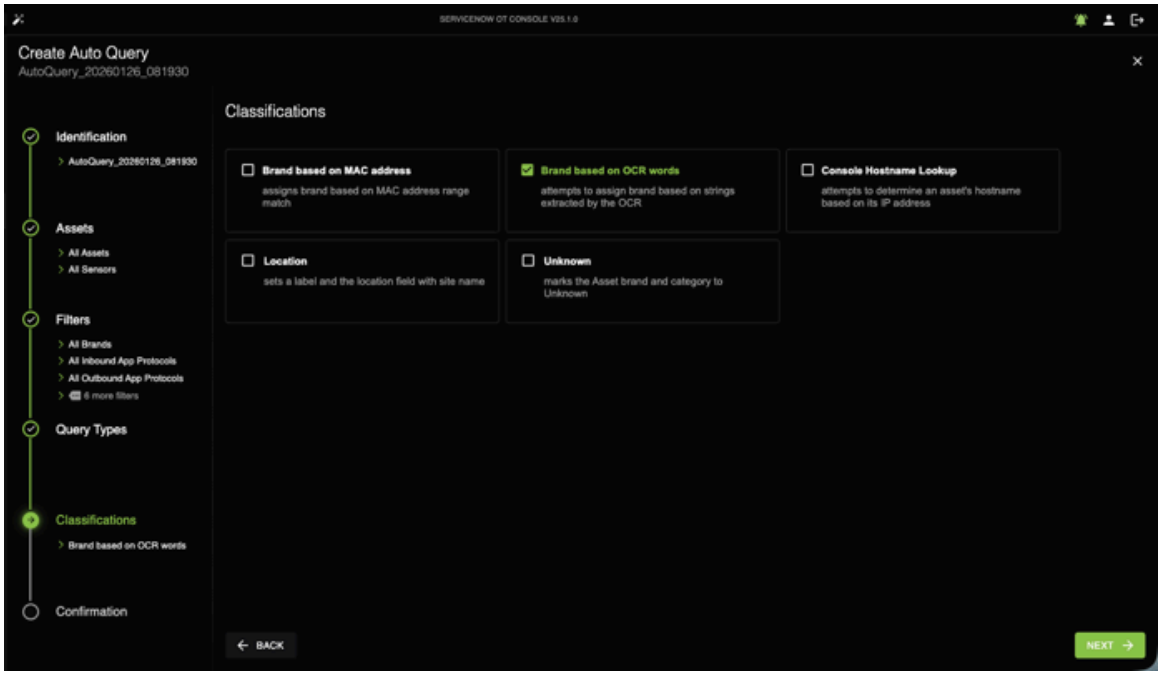
- **MelSecQ** - Query the Mitsubishi MELSEC-Q Series
- **Moxa** - Query to read the Moxa ICS setting
- **IPC-UA Deep** - Retrieve info from an OPC-UA target
- **ProfiNet DCE/RPC EPM** - Performs ProfiNet DCE/RPC EPM lookup requests
- **ProfiNet DCP** - PLC protocol often used for communicating with Siemens devices; this protocol is newer than S7. NOTE: Since this is a layer 2 scan it may return more results than selected.
- **SSL/TLS Certificate** - Query server to retrieve information about served SSL/TLS certificates
- **WMI** - Query Windows OS devices using Windows

11. **Optional:** You can set up the Auto Query scan to include all open ports.
To do this, select both or either the **UDP Port Enumeration** and / or **TCP Port Enumeration** (highlighted in the previous image) from the Advanced Query Types. Each scan determines all open ports for their two respective protocols.

> **Note:** For these query types to be available, verify your ScanScripts.json driver is up to date; if not, upload the latest version of this driver. For information, see Edit the Query Driver on Metadata tab.

12. Select **Next**
13. **Optional:** In the Classification section, select from the following.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- **Brand based on MAC address**: Assigns brand based on MAC address range match.
- **Brand based on OCR words**: Attempts to assign brands based on strings extracted by the OC. Fuzzy word search is supported.
- **Console Hostname Look up**: Attempts to determine an Asset's hostname based on its IP address.
- **Location**: Sets a label and the location field with Site name.
- **Unknown**: Marks the Asset brand and category Unknown.

14. Select **Next**.
15. In the Confirmation section, set the schedule, recursion, and duration.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

16. Select **Next**.
17. Select the **Create Auto Query** button.

Result
The query is added to the Auto Query page.

Create an Auto Query ignore list

Create an Auto Query to exclude specified asset IP addresses from receiving scanning traffic.

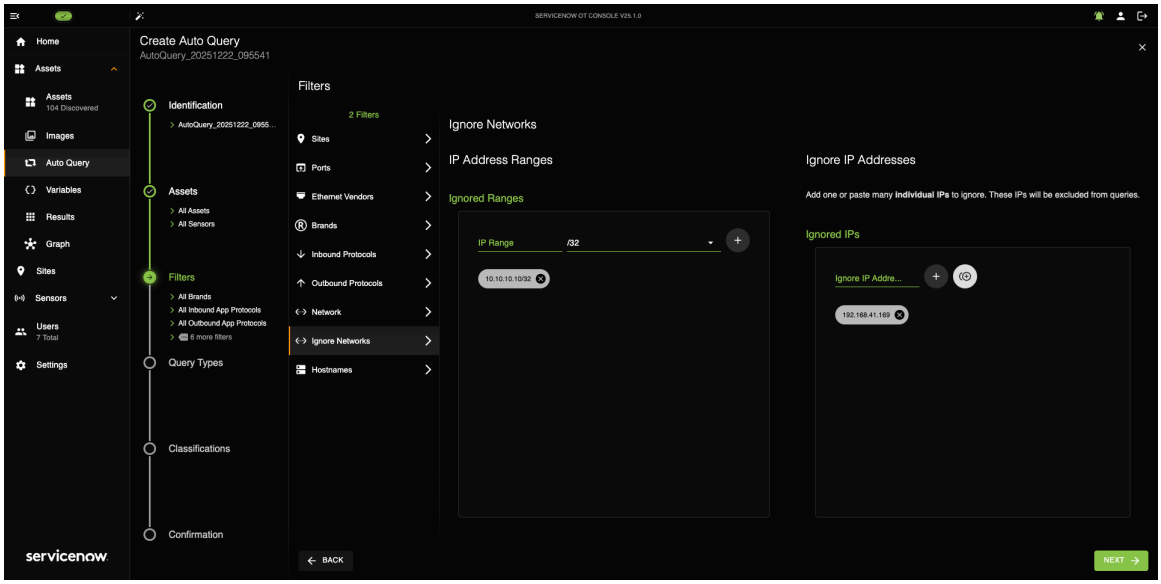
Before you begin
Role required: admin

Procedure
1. Navigate to the Auto Query page.
2. Select the add icon  .
3. In the Identification section, add the Auto Query name in the **Auto Query Name** field or use the generated name.
4. Select **Next**
5. In the Assets section, select the desired assets and targets.
   The Assets section displays a choice of All Assets, New Assets Only, Incremental, Asset Discovery, and Asset Discovery & Query.

   When the Query is set to use **All Assets**, then the Assets that are marked as ignored, are excluded from the list of targets.

   The Targets section lists All Sensors, Specific Sensors, and Auto Targeting.
6. Select **Next**
7. Specify any filters in the Filters selection.
   You can specify Sites, Ports, Ethernet Vendors, Brands, Inbound and Outbound Protocols, Networks, Ignore Networks, and Hostnames.
8. To create the ignore list, select the Ignore Networks filter.
   - To ignore an IP Address Range, enter an IP Range in the IP Address Range section, and select the add icon  .
   - To ignore one individual IP address, enter an IP address in the Ignore IP Address section.
   - To ignore multiple IP addresses, select the multiple selection icon  in the Ignore IP Address section, and use commas to separate the entries.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



9. Select **Next**
10. In the Query Types section, select as many types needed from one or both the Simplified Query list or the Advanced Query list.
11. In the Classification section, if you choose to, you can select from the following.
    - **Console Hostname Look up**: Attempts to determine an Asset's hostname based on its IP address.
    - **Location**: Sets a label and the location field with Site name.
    - **Unknown**: Marks the Asset brand and category Unknown.
12. Select **Next**
13. In the **Confirmation** section, set the schedule, recursion, and duration.

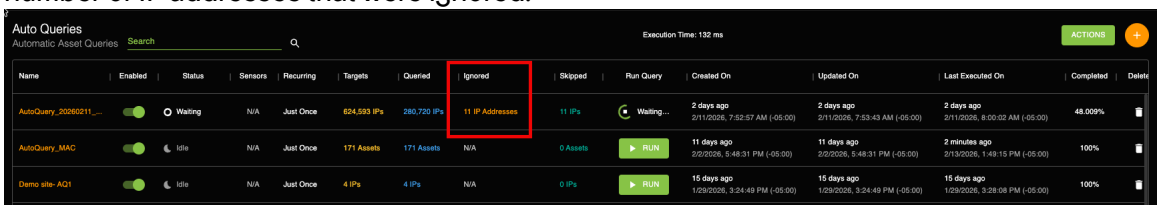


14. Select the **Create Auto Query** button to create the Auto Query ignore list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result

The Auto Query results are added to the Auto Query page. The **Ignored** column displays the number of IP addresses that were ignored.



Edit an Auto Query

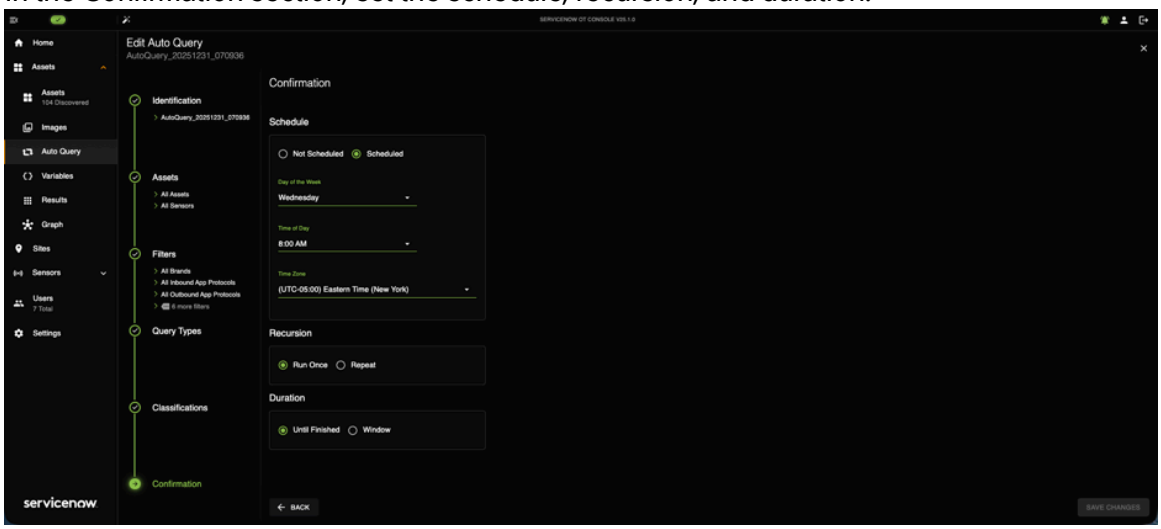
Edit an Auto Query to change or add parameters to your scan.

Before you begin

Role required: admin

Procedure

1. Navigate to the Auto Query page.
2. Select the query to be edited.
3. Step through each section in the Edit Auto Query view.
4. Change the settings that you want to change in the Assets, Filters, Query Types, and Classifications sections.
   If needed, select the X icon in the right-hand corner of the screen to return to the Auto Query list and discard your changes.
5. In the Confirmation section, set the schedule, recursion, and duration.



6. Select **Save** to save your changes or select **Cancel** to discard your changes

Create a Quick Scan

Create a **Quick Scan** from the Auto Query page.

Before you begin

Role required: admin

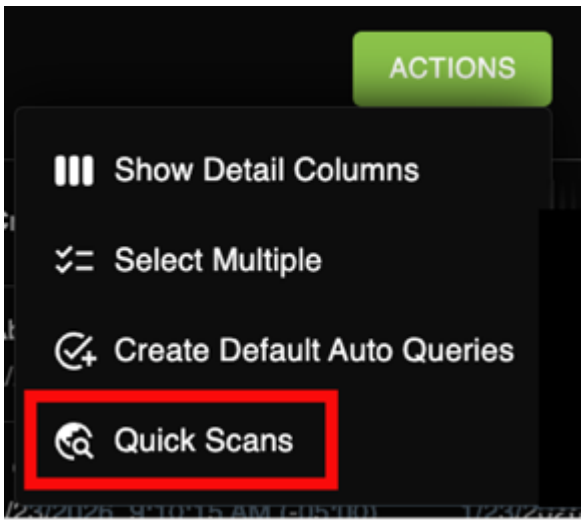
About this task

A Quick Scan has fewer options to choose from, but it also runs quickly at approximately 5 minutes. After the scan runs, select the View Results in the Results column.

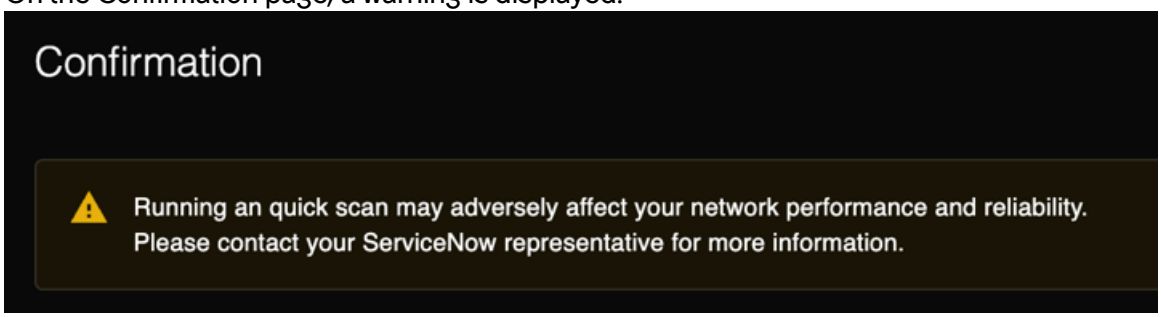
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to the Auto Query page.
2. Select the **Action** button.



3. From the Action drop-down menu, select **Quick Scans**.
   The Quick Scans page opens.
4. Select the add icon .
   Fill in each step and then select the **Next** button to move to the next step.
5. In the **Identification** field, add a unique name or use the one provided.
6. From the available selections, select a **Target**.
   Target selection includes:
   - **Assets**: You can select more than one and search for an Asset from the list.
   - **IP Addresses**: You can add one or more IP addresses to scan.
   - **IP Address Ranges**: Enter an IP Range. Select the add icon to add additional IP ranges.
7. In the **Sensors** step, select the box next to one or more listed Sensors.
8. Select a **Scan Type**.
   You can choose from the Simplified Query Type selection or toggle the **Advanced** button and select from the advanced query types. See the Auto Query page for additional information about Query Types.
9. On the Confirmation page, select the **Run Quick Scan** button to start the scan.
   On the Confirmation page, a warning is displayed.



Variables

The Variables page provides a list of currently available variable sets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Variable overview

The Variables page displays the available Variable sets on your system. It provides a Search Variables field above the variable list.

You can also create new variable sets. Variables are used for Auto Query scans and can be associated to a specific Site.

The columns on the page are:

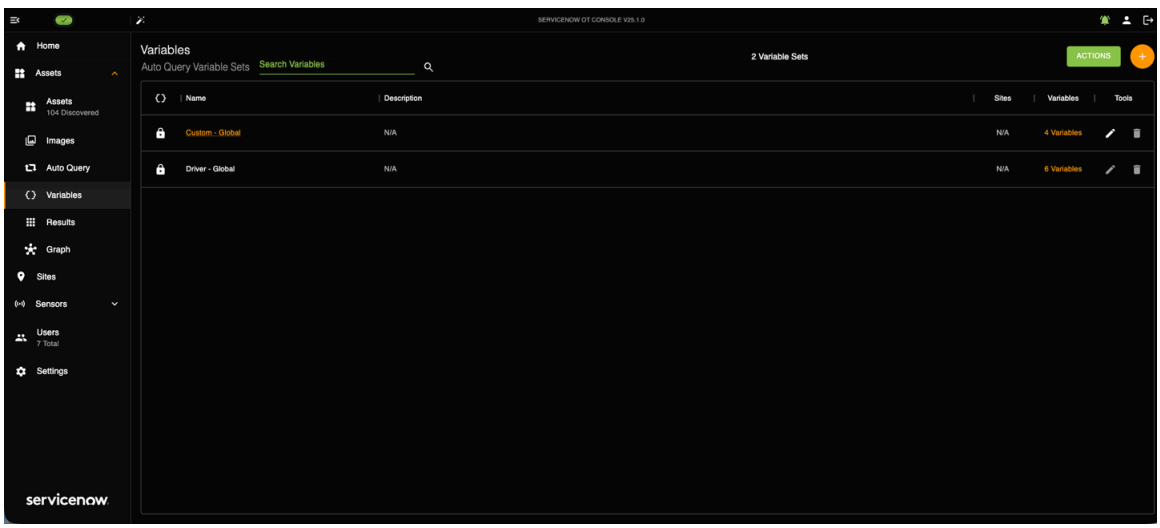
- The bracket dot icon and lock icon appear in the row next to the variable listing. When the bracket-dot symbol appears green next to the variable's name, the variable can be used for auto queries. When white, the variable can't be used for auto queries. The green lock indicates that the variable password is encrypted.

  Note: Encrypted Variable values in Variable Sets are obscured.

- Name
- Description
- Sites display the name of the site to which the variable is associated.

  Note: A Site can only be associated with a single Variable set, but a Variable set can contain many variables.

- Variables (number of variables)
- Tools
  - Select the pencil icon to edit the variable set.
  - Select the trash can icon to delete the variable set.



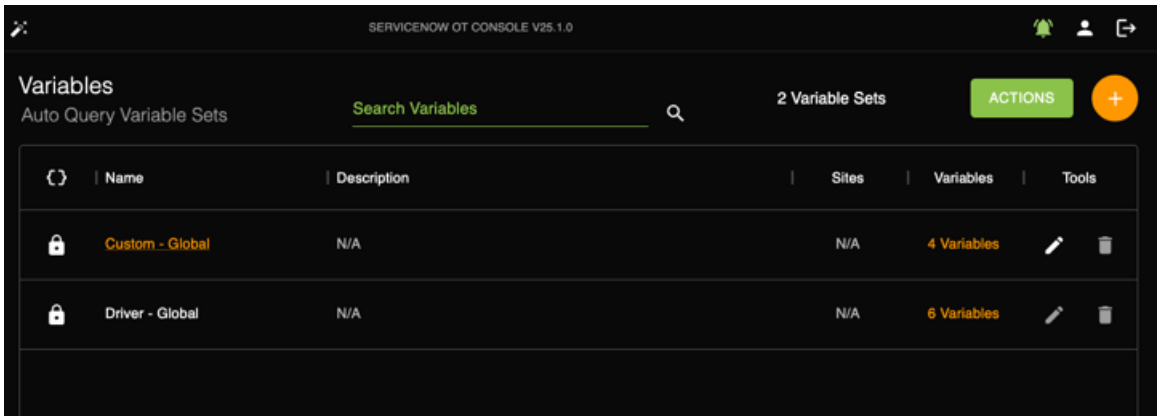
Special Variable sets

There are the following special variable sets:

- Custom - Global
- Driver - Global

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Custom-Global variable set can be edited by a user while the Driver - Global is read-only. The Custom - Global variable sets can be used to override indirectly the Driver - Global variable sets.



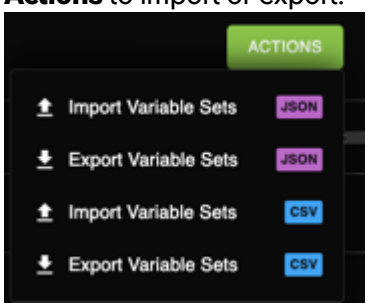
You can use variable sets (Custom - Global or Site-specific sets) to override a Variable set. See Edit a Variable set or Create a Site-specific Variable set to use with Auto Query for more information on editing a Variable set.

Query Behavior

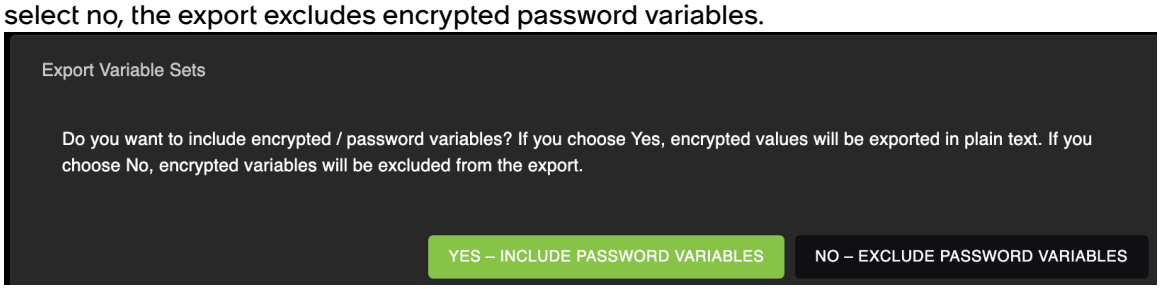
During a query, the query configuration is reviewed to see which Sites are being targeted. The query then searches to see if any Site-specific variable set override is defined. If no override is defined, it then searches to see if any Custom - Global override is defined. If it doesn't find a custom override, the query uses the default variable set from the Driver - Global.

Importing or exporting Variables sets

You can import or export variable sets. You can select either the JSON or CSV formats. Select **Actions** to import or export.



When you export Variable sets in either JSON or CSV format, you're prompted to include encrypted password variables. If you select yes, the values are exported as plain text. If you select no, the export excludes encrypted password variables.



If the encrypted password is exported as plain text, it is no longer hidden and secure.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Encrypted Variable values in Variable Sets are obscured. Encrypted values display as dots when set to encrypted.



Note: For information on creating a Site-specific Variable set, refer to Create a Site-specific Variable set.

Create a Variable set

Create a Variable set for an Auto Query scan created in the Discovery Console for OT.

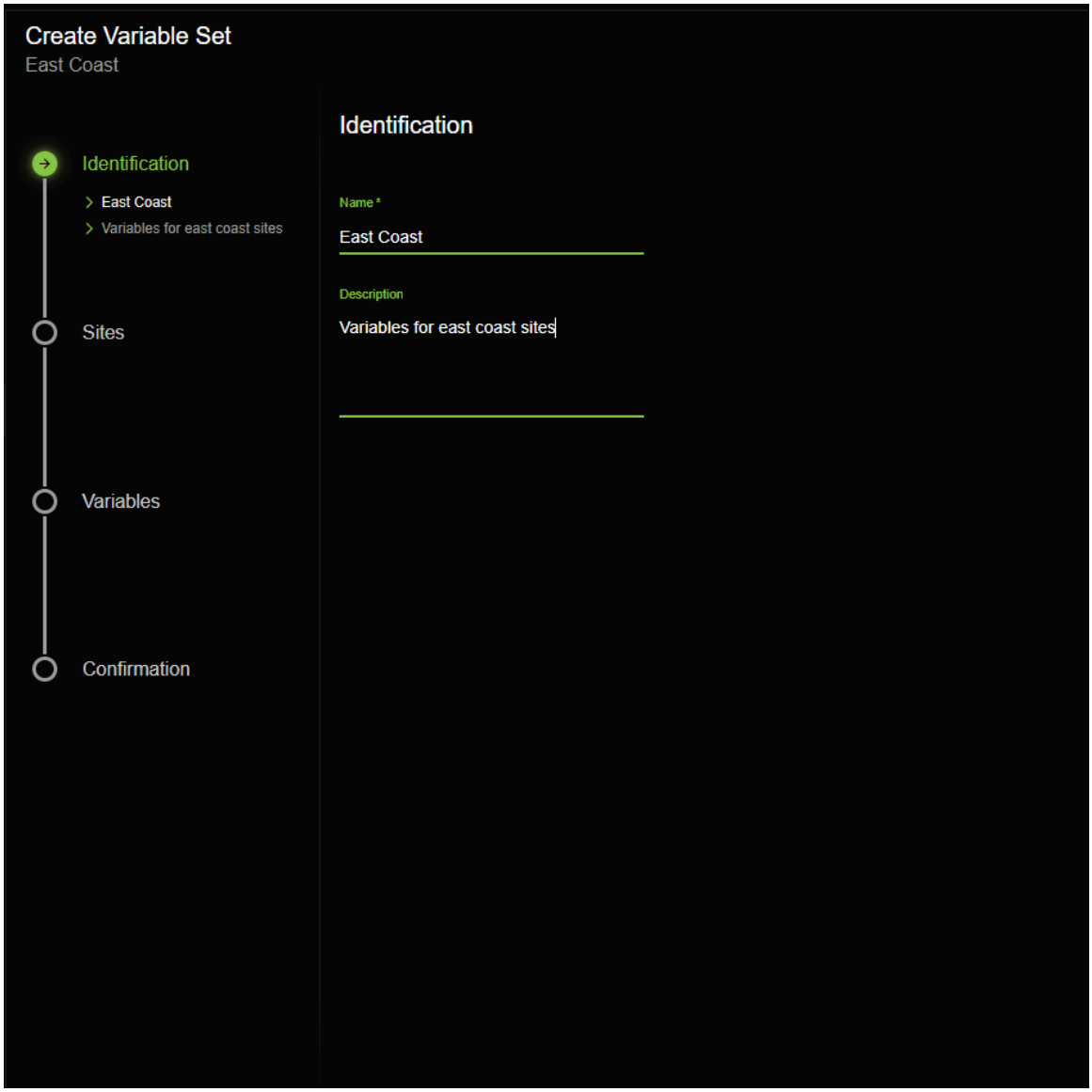
Before you begin

Role required: admin

Procedure

1. In the Console, navigate to **Assets > Variables**.
2. Select the add icon .

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. On the **Create Variable Set** page, add the necessary information and then completion, select **Next**.
4. **Identification**: Enter information in the fields for the Variable name and description.
5. **Site**: In the Select Sites section, put a check mark in the box next to a site name (if available). Using the icons under the list allows you to select all or deselect all sites .
6. **Variable**: Select from the list of available Variables.
7. **Confirmation**: Confirm to create the Variable.

Result

The new variable appears in the Variable list.

Note: A Site can only be associated with a single Variable set, but a Variable set can contain many variables.

Edit a Variable set

Edit a Variable set for an Auto Query scan created in the Discovery Console for OT.

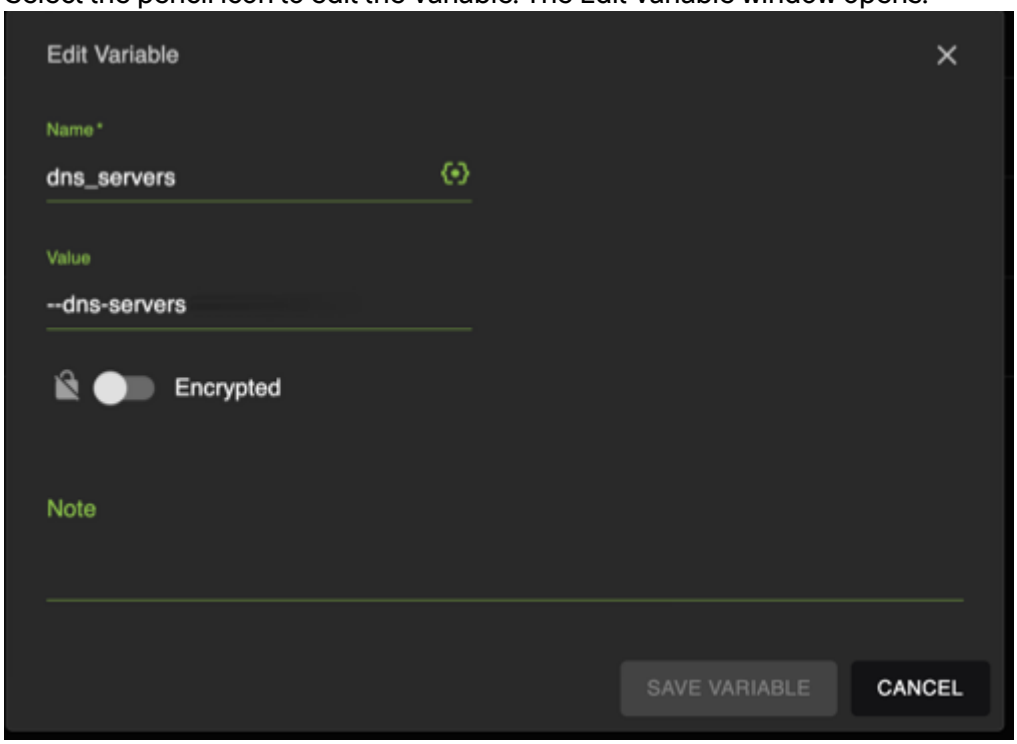
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

Procedure
1. Navigate to the Variables page.
2. Select a Variable set.

   Note: Editing the Custom - Global variable set allows you to globally override variable values defined in the Driver - Global variable set.

3. Select the pencil icon for the Variable.
   The Edit Variable Set view opens.
4. Edit parameters as needed.
   a. **Identification**: Edit the name and description of the Variable.
   b. **Sites**: Select a different site from the original selection if needed.
5. In the Variables section, you can edit or delete the variables as needed.
   Select the pencil icon to edit the Variable. The Edit Variable window opens.



6. To hide the value of a Variable, slide the toggle next to Encrypted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: Encrypted Variable values in Variable Sets are obscured. Encrypted values display as dots when set to encrypted.



Create a Site-specific Variable set to use with Auto Query

Create a Site-specific Variable set for use in Auto Queries.

Before you begin
Role required: admin

About this task
Create a Site-specific Variable set to define query Variable values for use in Auto Queries. You can use the Variable set as a credential for your Site.

Note: A Site can be associated to only one Variable.

Procedure

1. Navigate to the Variable page in the Console.
2. Create a Variable as described in Create a Variable set.
3. When you create the variable, select a Site to associate it.
4. Create an Auto Query as described in Create an Auto Query.
5. In the Filter section of the query, select the Sites filter.
6. From the list of sites, select the site to associate to your variable.
7. Complete creating the query.
8. Run the Auto Query that you created.

Result
Your Site is queried and associated to the Variable.

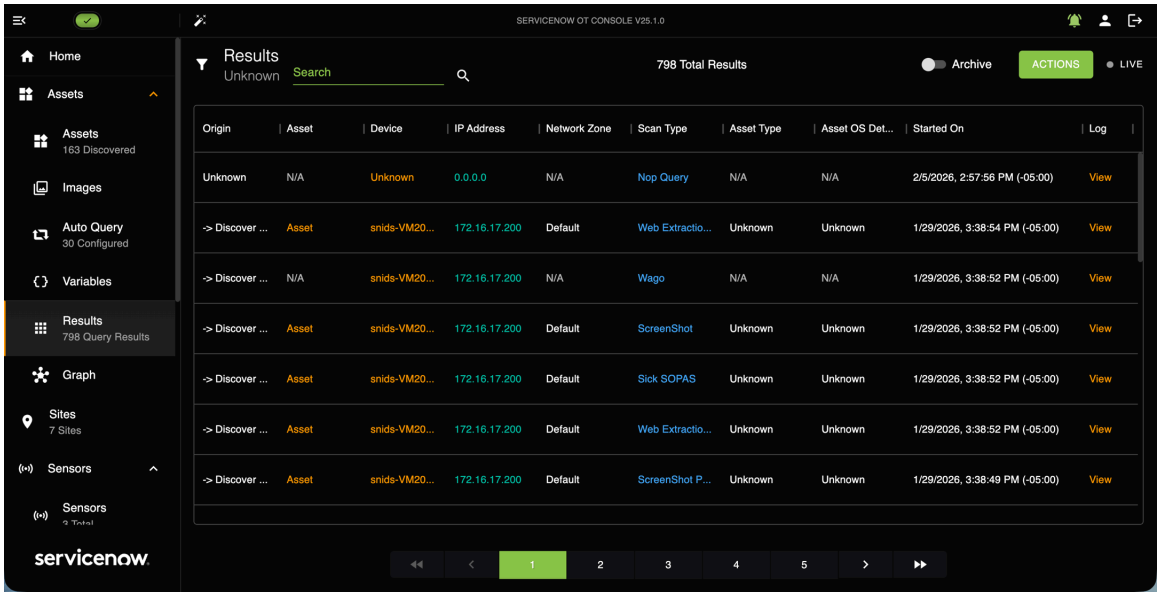
Results page

The Results page provides the results from your queries in the Discovery Console for OT.

The Results page contains a list with all the scan results in the system. Each scan is displayed along with the associated Device, IP Address, Network Zone, Scan Type, Asset Type, Asset OS Details, Started On, and Log. The following image shows an example of the Results page.

Note: You can't export RAW XML results if your Console license is invalid (absent or expired).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

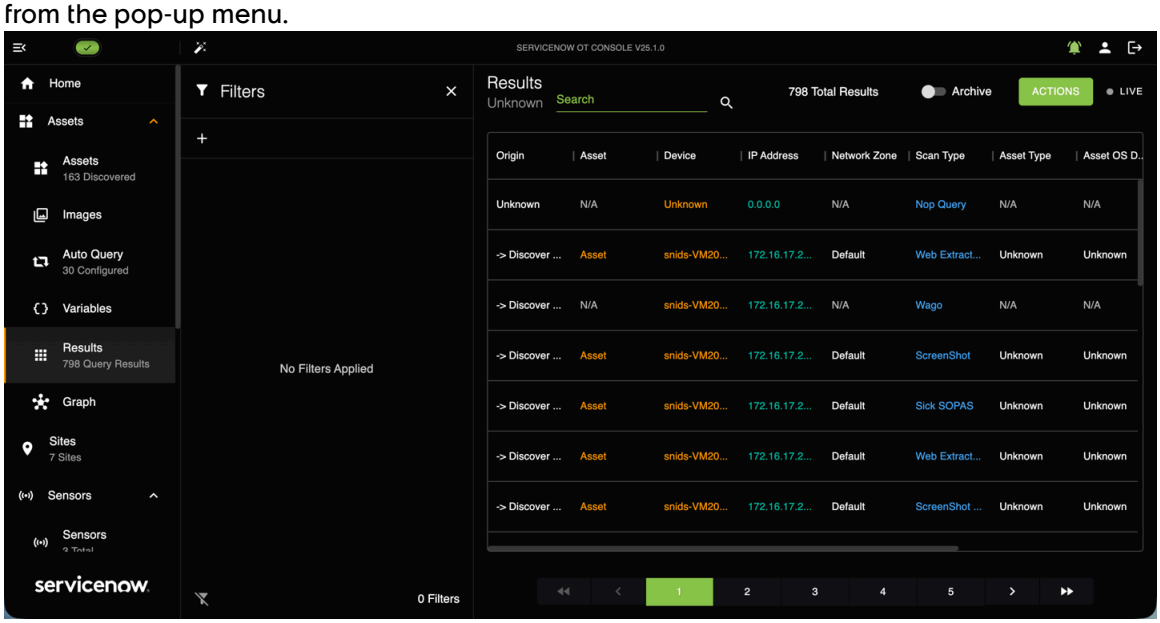


To access the Results page, navigate to **Assets > Results**.

To find a specific scan, you can enter text into the Search bar on the top of the page under the Results heading.

Result filters

Use the filter panel to select which queries display in the results list. To filter the scan results, select the Add Filter icon + in the filter panel. Put your cursor in the filter field and select a filter from the pop-up menu.



See Filter results for more information.

Viewing results

On the Results page, you can view details of a result by selecting column entries.

Asset

Selecting an asset name in the Asset column opens the asset editing window. This view has three tabs, Details, Image, and Module On the Details tab you see

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Identification, Classification, Timeline, and other detailed sections. You can select Edit if you need to change any of these settings. If there is an image attached, it displays in the Detail and Images tabs. The Modules tab displays specific information about system modules, such as if the asset is a CPU or PLC, and the manufacturer's name.

Appliance

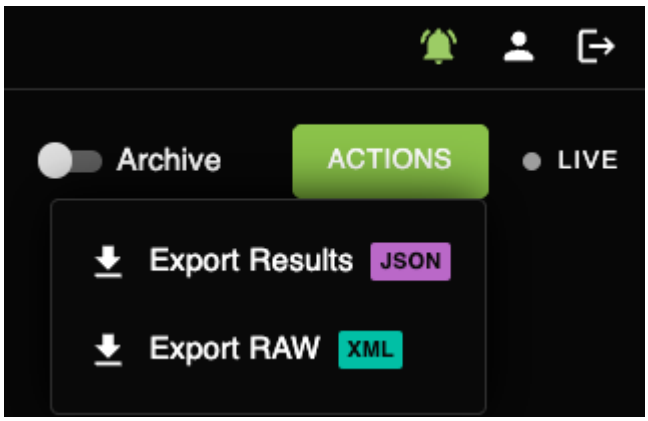
The Appliance column lists the name of the Sensor or Collector used during the query. Selecting the name from this column allows you to edit the query appliance's information and configuration.

Log

Select View in the Log column and the query log displays. You can copy the log for later use and for troubleshooting.

Action button

The Results page **Action** button lets you export the scan results. You can **Export Results** in JSON format or **Export RAW** in XML format.



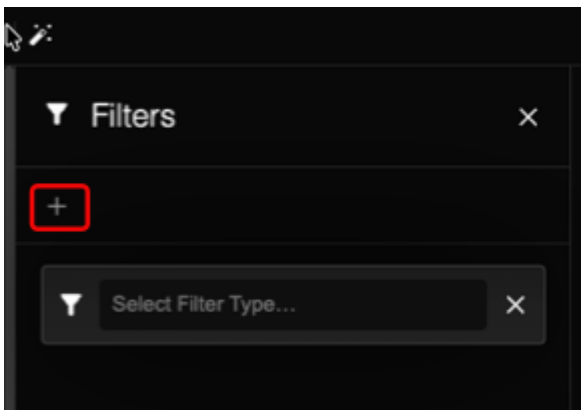
The RAW data format is useful for debugging and verification.

Filter results

The Results page provides a filter to find specific types of queries of information.

Filtering the query results

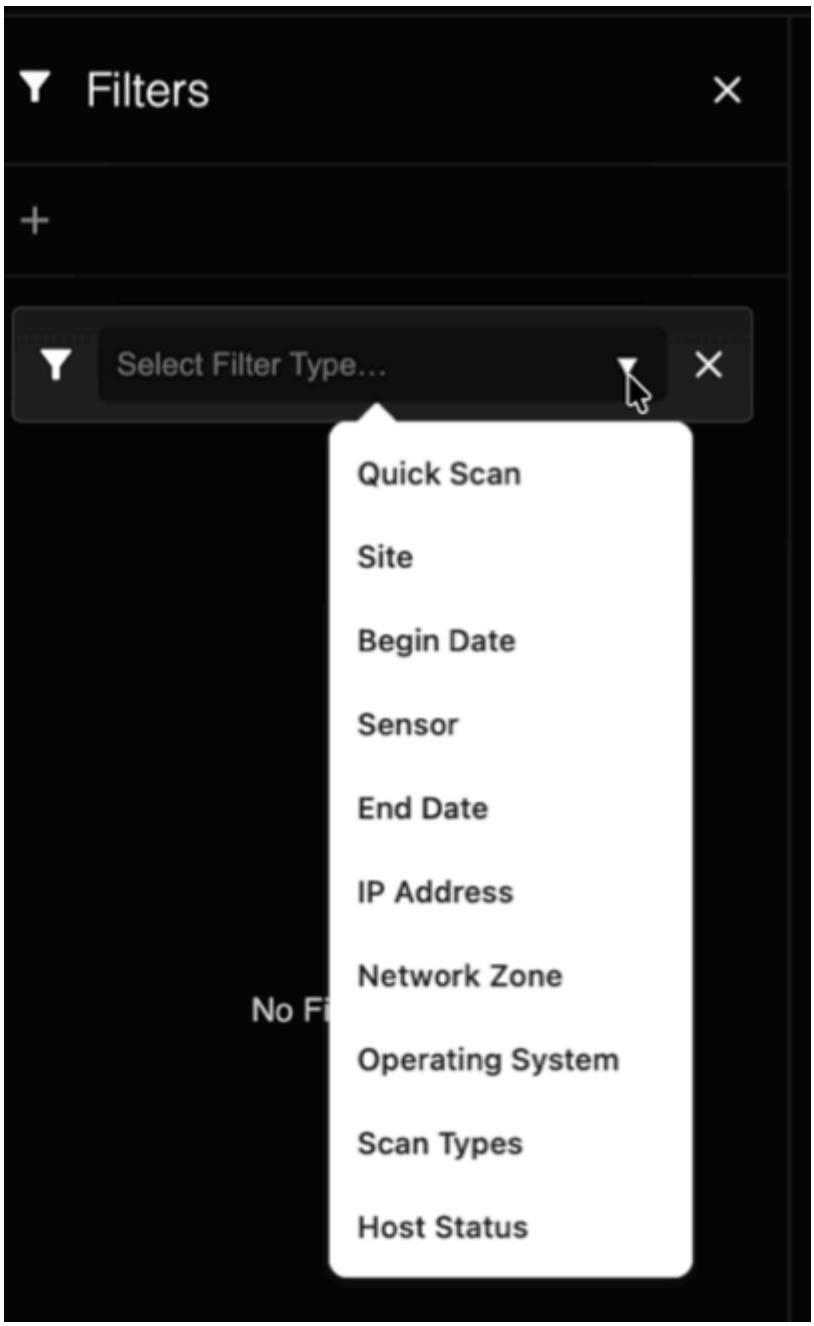
Much like the Assets page, the Results page provides a filter to the left of the Results list. To open the Filter type list, select the plus sign + under the Filter header. This opens the drop-down selection field.



The menu drops down and you can select from the following list.

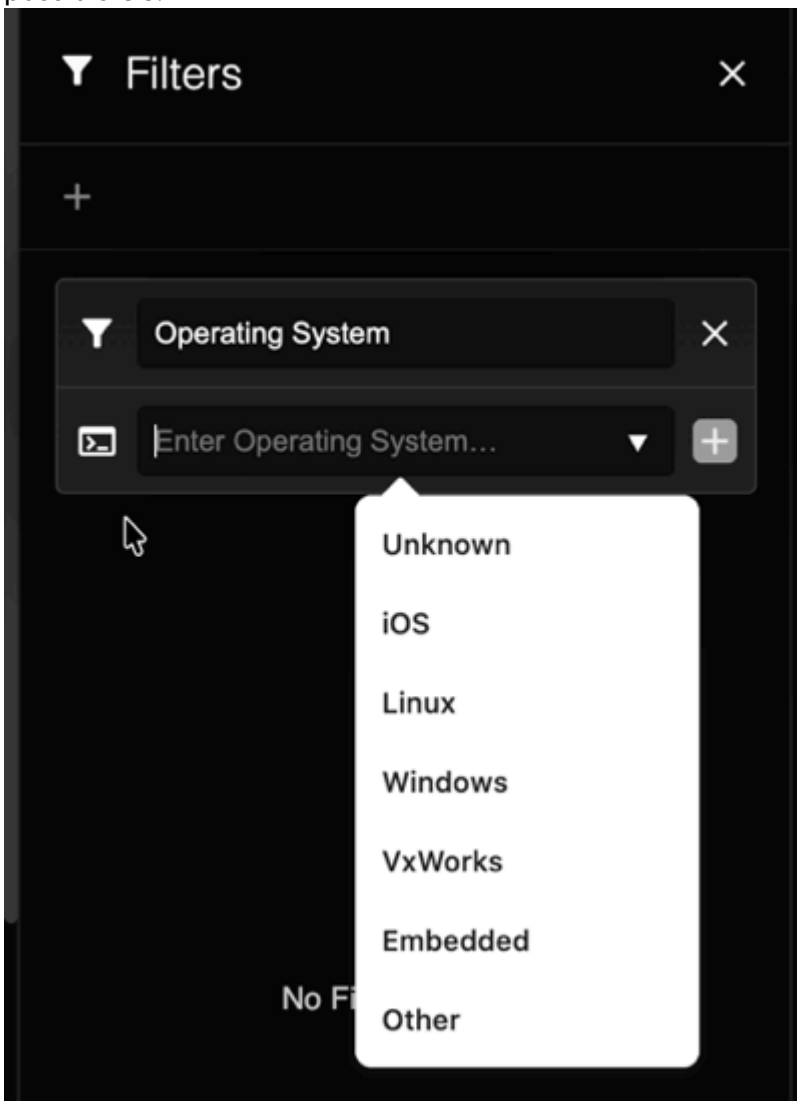
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Quick Scan
- Site
- Begin Date
- Sensor
- End Date
- IP Address
- Network Zone
- Operating System
- Scan Types
- Host Status



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you select Operating System, for example, another drop-down menu opens with a list of possible OS.



After you have made your selection, any query that matches the filter displays on the Result page.

Filter results for Host Status

Filter your query results by Host Status. Verify whether devices were reachable when the query was executed.

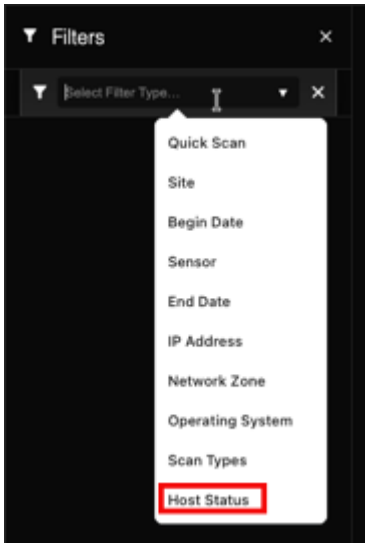
Before you begin

Role required: admin

About this task

In the Scan Results filtering types, the **Host Status** enables users to view query results based on whether the queried host was **Up** or **Down**. This filter is derived from the **Nmap XML status field** inside the Raw scan output.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: This filter is based on raw scan output and does not depend on scan type. If a scan output does not contain a host `status state="up|down"` field, it does not match the Host Status filter.

Using the Host Status filter helps to quickly narrow results such as:

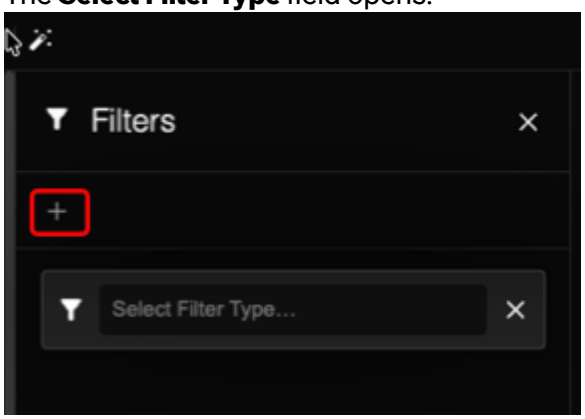
- Shows only reachable devices (Up) to review open ports or services.
- Shows only unreachable devices (Down) to troubleshoot network issues, firewall rules, wrong IPs, or powered-off devices.

Raw data is useful for debugging and verification because:

- Reason field: Raw data confirms why a host was marked Up/Down.
- Good for investigation: Raw data shows what the Nmap actually returned.
- Script validation: Raw data helps validate scripts when scan parsing or mapping doesn't show expected information.

Procedure

1. Navigate to the Results page.
2. In the Filter panel, select the plus icon. +
   The **Select Filter Type** field opens.



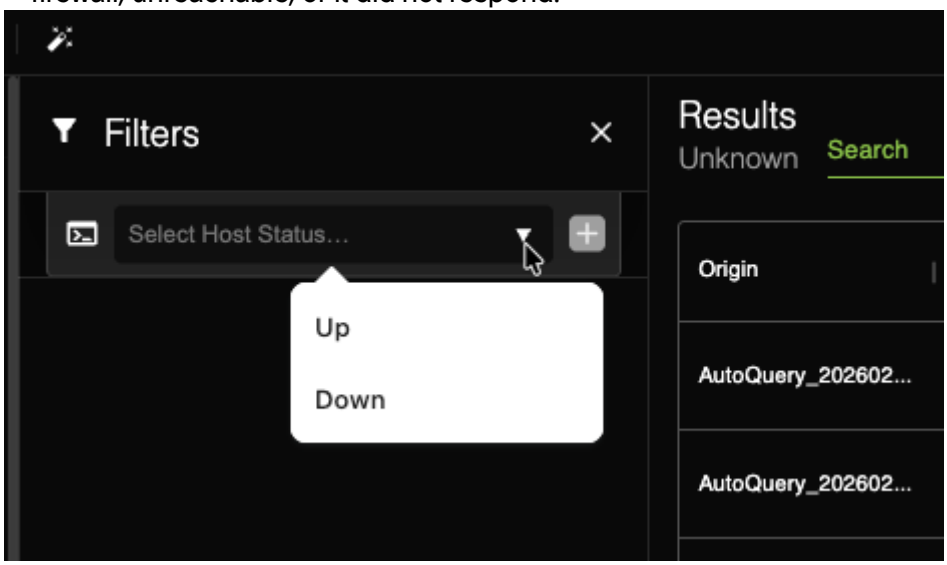
3. In the Filter field, select Host Status from the drop-down menu.
   The **Select Host Status** field opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select from the pop-up choices one of the following.

   Note: **Up/Down** in this instance means the **host status from the scan result (Nmap)** for that IP during that query run.

   - **Up** means the target asset responded, that is, the appliance was able to reach it and also got a response back.
   - **Down** means the target asset did not respond; this could mean it is offline, blocked by firewall, unreachable, or it did not respond.



5. Using the Host Status filter helps to quickly narrow results:
   - Showing only **reachable assets** (Up) to review open ports/services.
   - Showing only **unreachable assets** (Down) to troubleshoot network issues, firewall rules, wrong IPs, or powered-off devices.
6. Raw data is useful for debugging and verification because:
   - Raw data confirms why a host was marked Up/Down (reason field).
   - Raw data shows what Nmap actually returned (good for support/investigations).
   - Raw data helps validate scripts when querying/mapping doesn't show expected information.

Appliances page

The Appliances page displays active appliances in the Discovery Console for OT.

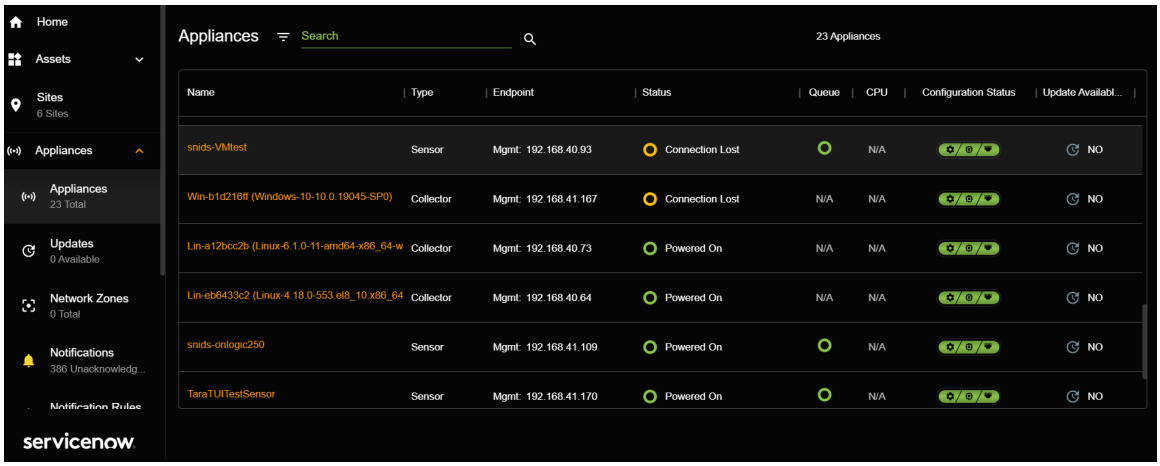
Appliances

The Appliances page displays the current Sensors and Collectors that have run or are running your queries. The information displayed includes the following:

- Name
- Type
- Endpoint
- Status
- Queue

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

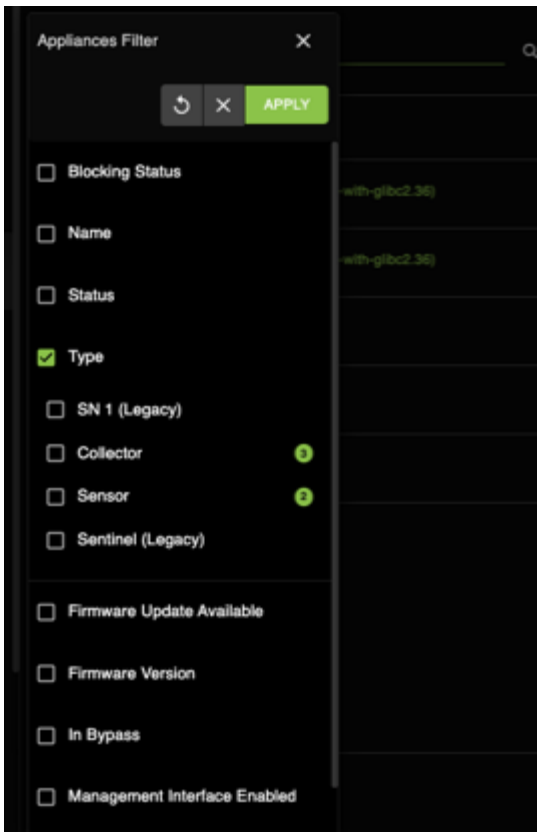
- CPU
- Configuration Status
- Update Available?



For more information, see Edit an Appliance.

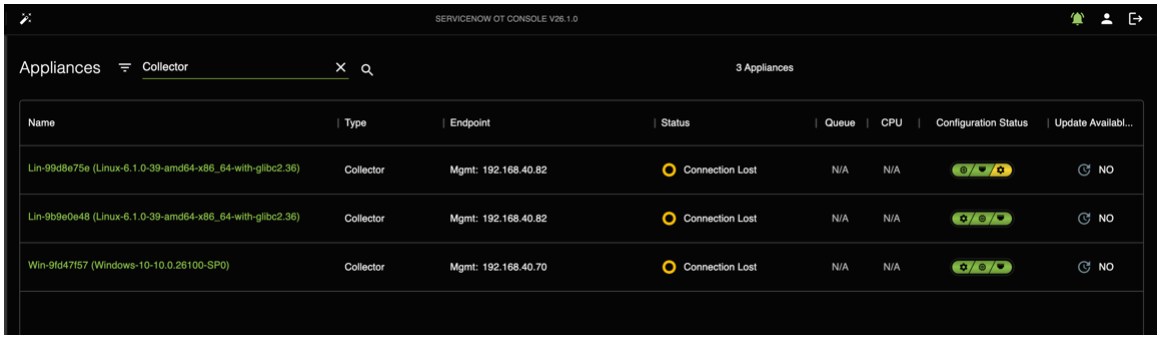
Search by type

You can search for a type of appliance by entering the type in the Search field. Or you can open the Filter and select by the available labels. For example, if you want to view just the Collectors, you can type Collector in the Search field. You can also check the box next to Type in the drop-down Search menu.



Then choose Collector. The Appliances list now shows only the current Collectors.

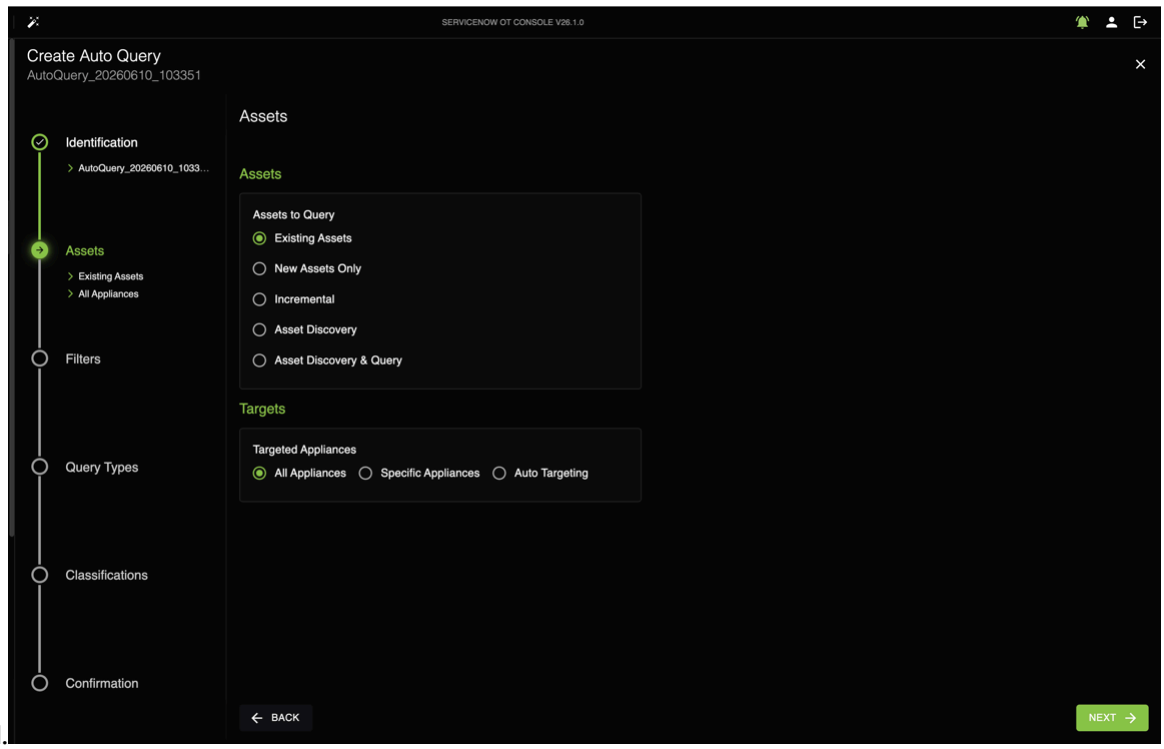
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Using Appliances in Queries

The Discovery Sensor for OT executes the query to discovery assets and creates the OT environment inventory. The OT Discovery Collector is used to discover assets within segments of the OT network where a Sensor can't reach. It is deployed deep within the network zones in your OT environment.

When you create an Auto Query in the Console, you can choose specific Appliances in the Assets section. When choosing Assets for the query, you can assign the Target to all appliances, specific appliances, or auto targeting. If you select **Specific Appliances**, you can select the appliances you want from a provided list. One restriction is that you must select at least one Sensor from the list as well.



For more information, see Auto Query page and Create an Auto Query.

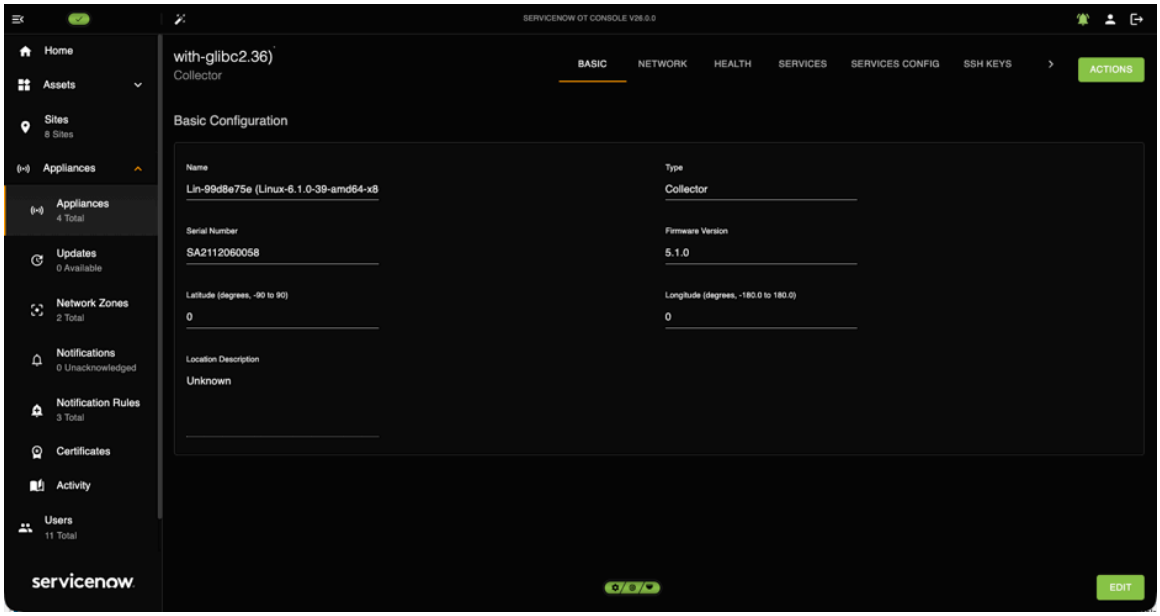
Edit an Appliance

This section describes what information that is available and that is setup on an Appliance record

Edit an Appliance

To edit any appliance, select the Name of the appliance. The appliance record opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The appliance view has tabs with additional information and options. Move to a tab and then select the **Edit** button to edit any of the appliance settings. Select the **Save** button to save your changes or **Cancel** to discard them.

The following sections describe the available appliance information shown as tabs in the record.

Basic

This tab displays the basic configuration information for the appliance. The configuration includes the **Name**, **Type**, **Serial Number**, and **Firmware Version**. It also contains user-definable location information including fields for **Latitude**, **Longitude**, and **Location Description**.

Network

The **Network** tab shows the network settings as they're currently configured for the appliance. Each field is described in the following list:

- **Console Endpoint**: Shows the IP address of the Discovery Console for OT that the appliance is configured to use.
- **Appliance Gateway**: Shows the IP address assigned to the appliance that is used to route traffic between networks.
- **Management Interface**: Connects the appliance to an out-of-band network for communication with the Discovery Console for OT.
  - **Management Endpoint**: Sets the IP address for the Sensor which it uses to communicate with the Discovery Console for OT.
  - Management Subnet: Sets the subnet mask/Classless Inter-Domain Routing (CIDR) for the appliance communication with the Discovery Console for OT.
  - (Optional) **Management VLAN**: Specifies the VLAN identifier that the management interface uses to tag network communications for participation in VLAN segregated networks.
- **Span Interface**: When enabled, allows the appliance to collect all network traffic received on the ETHERNET 1 port. This allows the IDS to collect data from the network. When disabled, the appliance can't perform any data collection.
- **Networks Monitored by Arpwatch**: Lists networks that are being monitored by Arpwatch.
- **Ethernet Interfaces**: Lists all Ethernet Interfaces for the appliance. The list includes the Interface name and the MAC Address for each one.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Health

The **Health** tab enables you to view graphs reflecting trends in CPU, memory, disk utilization, and temperature and network input and output over time. You can set the data and time you want the CPU activity to reflect.

Services

You can configure specific services that run on an appliance. Currently, you can use this feature to enable or disable the SSH service on an appliance. Select the **Edit** button and then select the toggle to turn the SSH service on or off. This setting provides the **Status** and **Updated On** fields for the SSH service. Similarly, you can enable or disable the Log Streaming and Web Management services and view the corresponding **Status** and **Updated On** fields. The SSH service is enabled by default on all Sensors to facilitate post-installation configuration.

Services Config

The **Services Config** tab includes the **Log Streaming Service**, and the **Web Management Service**. You can use the Log Streaming Service to stream logs from appliances to the Discovery Console for OT. This service also retains logged information for a longer period, which can assist in quicker customer issue resolution.

To set the **Syslog Severity Level** for the Log Streaming Service, select **Edit** and use the drop-down menu to select the severity. You can select the minimum log severity, Informational, to include in the streaming for the appliance. Selecting the Debug level results in the most information being logged.

The data stream isn't viewable in the Console UI. The Console only provides the ability to enable or disable the service and set the log severity level. Streamed log information is retained on the Console for 30 days.

You can use the Web Management feature to reset the Web Management Service password on the appliance. To reset the password, select **Edit**. Enter a password in the **Password** field, enter the same password in the **Confirm Password** field, and then select **Save**. The **Status** and **Updated On** fields provide information about the Web Management Service on the appliance.

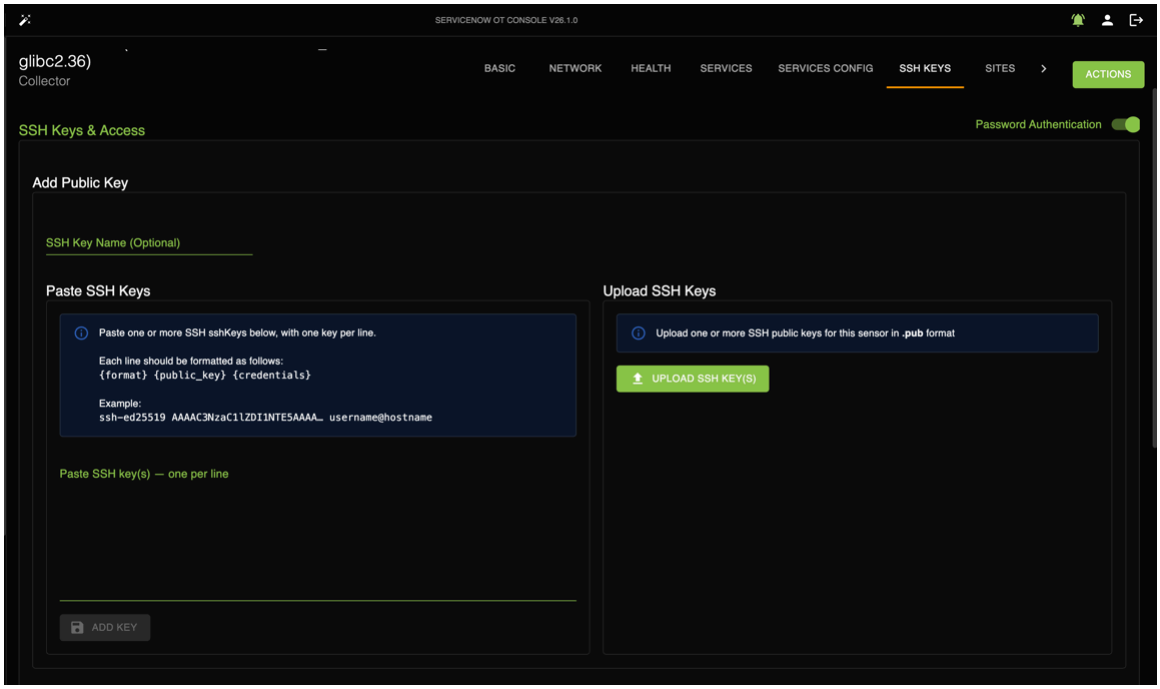
SSH Keys

On this tab, you can add public keys by listing the SSH key name in the **SSH Key Name (Optional)** field. You can also select **Paste SSH key(s) - one per line** and paste in keys. **Password Authentication** is enabled by default in the initial appliance install. To enable or disable the SSH password authentication, slide the toggle. You can also upload your own SSH Keys. The required format for a key is .pub.

Duplicate keys are automatically removed, so the same SSH key appears only once, even with small formatting differences like extra spaces.

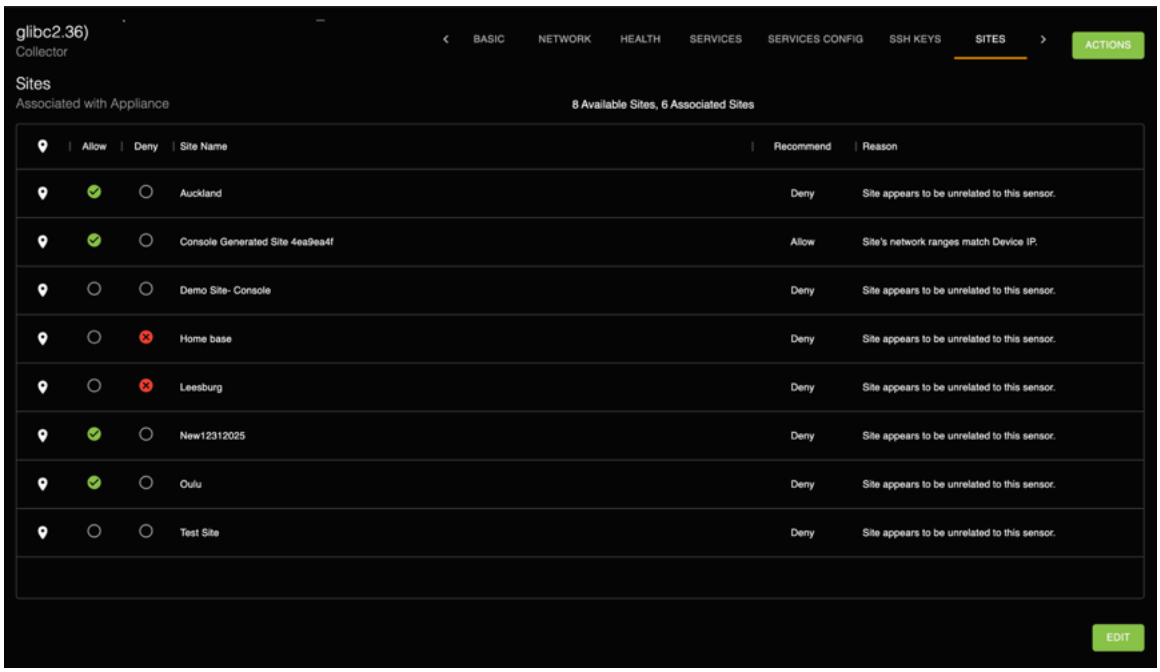
Note: As a safety feature that allows continued SSH access, disable **Password Authentication** only if you have uploaded at least one SSH public key to the appliance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Sites

The **Sites** tab displays which sites are associated with the selected appliance record during an Auto Query. The Allow/Deny setting indicates whether the appliance is associated with a listed Site. The tab also displays the site name, recommended setting for that site, and the reason for the recommendation. A Deny recommendation means the Site does not appear to be related to the appliance. An Allow recommendation means the Site's network ranges match the Device IP. Select the **Edit** button to change the Allow/Deny settings. Select the **Save Associations** button to save changes or **Cancel** to discard any changes.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

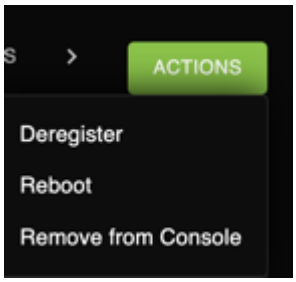
Status

This tab shows the current connection status of the appliance, including deployment status for basic configuration, network configuration, arpwatch networks configuration, policy, and firmware updates. Editing these settings is not available.

Actions button

The **Actions** button in the appliance record enables the following actions.

- **Deregister Device**: Deregisters the appliance from the Console. This action resets the network settings to factory defaults and removes the appliance from the Console.
- **Reboot Device**: Reboots the appliance.
- **Remove from Console**: Removes the appliance from the Console.



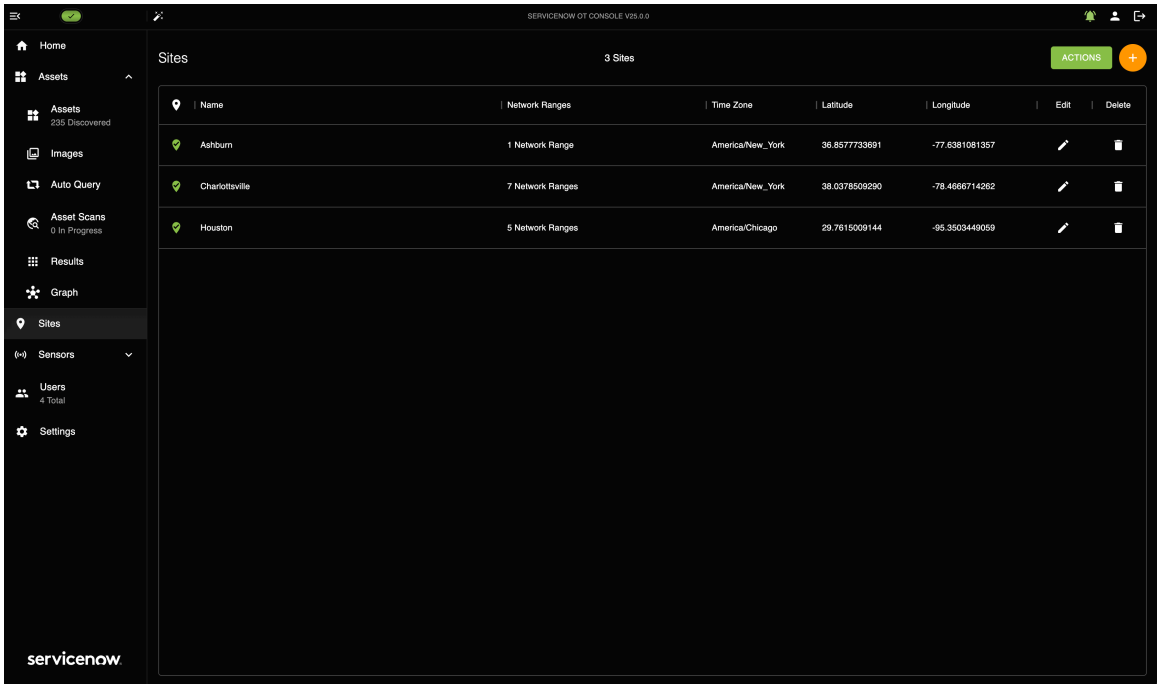
Sites page

A Site represents a physical location in your organization, such as a DATACENTER, office, or IoT site. Each Site includes location details, time zone settings, and network range configurations that determine which IP addresses the Console for scans during discovery.

Note: Sites is the starting step to group assets. All devices that are part of a given network range defined in the Site configuration are assigned to that site. If there are multiple Network Zones within the Site, these zones could be assigned to a Site for grouping purposes.

The Sites page contains a list of all the sites available in your Discovery Console for OT system. For each site, you can view the network range, time zone, latitude, and longitude. The following image shows an example of the Sites page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: You can't select the same IP Addresses for both the Include and Ignore selections for the Site without triggering an error.

Add a Site

Add a site to your Discovery Console for OT.

Before you begin

Role required: admin

Procedure

1. Navigate to the Sites page.
2. Select the add icon.
   The Site creation wizard opens.
3. In the Identification section, enter a unique name for your site.

   Note: The site name must be unique across your Discovery Console instance. Use a descriptive name that clearly identifies the location. For example, "Seattle_DataCenter" or "NYC_Office_Building_A".

4. Select **Next**.
5. In the Address section, add the physical address to your site.
   This information helps identify the site's geographic location for organizational purposes.
6. Select **Next**.
7. In the Location section, specify the geographic coordinates using one of these methods:
   a. Enter the latitude and longitude coordinates directly in the provided fields.
   b. Select a location on the interactive map to automatically populate the coordinates.
8. Select **Next**.
9. In the Time Zone section, begin entering the zone name in the Search field to quickly filter available time zones.

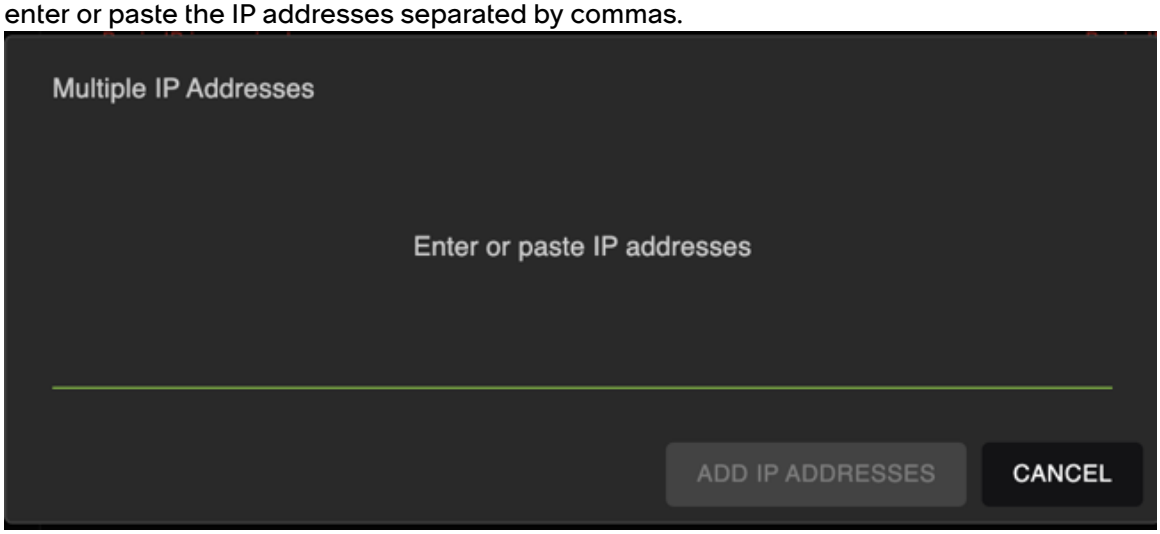
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Search filter displays all related Time Zones on the page.

10. Select the button next to the desired Time Zone, and then select **Next**.
11. In the **Network Ranges** option, select at least one range or a Network Zone that has at least one range.
    The Network Ranges configuration determines which IP addresses Discovery Console scans (including) and which it ignores during discovery operations for this site.
12. Add IP address ranges to scan:
    a. Under Include, select the **Begin IP** field and select or enter the starting IP address.
    b. Select the **End IP** field and select or enter the ending IP address.

    Note: The Console automatically prevents you from selecting the same IPs for both the Begin IP and End IP in both the Include and Ignore sections.

13. Add individual IP addresses to scan:
    a. Under Include, select the **IP Address** field, enter a single IP address, and select the add IP address icon .
    b. To add multiple IP Addresses at once, select the add multiple IP Addresses icon , and enter or paste the IP addresses separated by commas.



14. Exclude or ignore IP address ranges to scan:
    a. Under Ignore, select the **Begin IP** field, and select or enter the starting IP address.
    b. Select the **End IP** field and select or enter the ending IP address.
15. Exclude or ignore individual IP addresses to scan:
    a. Under Ignore, select the **IP Address** field, enter a single IP address, and select the Add IP Address icon .
    b. To add multiple IP Addresses to ignore, select the Add Multiple IP Addresses icon , and enter or paste the IP addresses separated by commas.

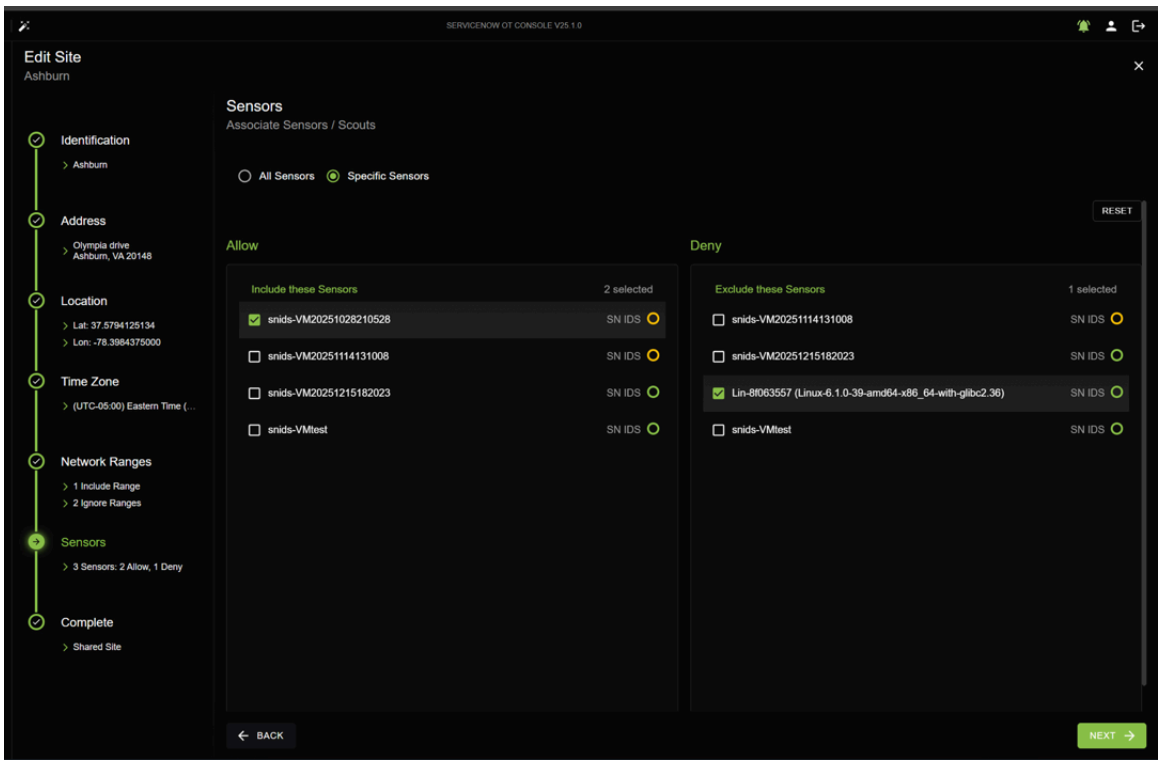
    Note: You can't include and ignore the same IP address. If you attempt to do so, the system displays an error.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

16. Include network zones:
    a. Under Include, select the **Network Zone** field.
    b. Select one of the Network Zones from the drop-down menu.
17. Exclude network zones:
    a. Under Ignore Network Zones, select the **Ignore Network Zone** field.
    b. Select one of the Network Zones from the drop-down menu.

> **Note:** The Discovery Console for OT automatically prevents conflicts. When you add a zone to the Include list, it is set to unavailable in the Ignore list, and vice versa. This confirms that each zone is assigned to only one list.

18. **Optional:** If you want to prevent overlapping IP address ranges, select the **Prevent Range Overlap** toggle.
    This option helps avoid configuration errors when multiple ranges are defined.
19. On the Sensors page, select Sensor by checking a box next to their name.
    You can select Sensors in the Allow and Deny sections; but don't select the same Sensor in both sections.



> **Note:** Sensors are online when the circle next to their name is green. A yellow circle indicates Sensors that are offline.

20. After configuring network ranges and zones, review the summary of information.
21. Review all settings, and then select **Create Shared Site**.

Result

The system creates the site and returns you to the Sites page where your new site appears in the list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Edit or delete a Site

Edit a site to update its information or delete a site that no longer exists on your Discovery Console for OT.

Before you begin
Role required: admin

Procedure

1. Navigate to the Sites page.

Edit a Site

2. To edit a Site, do the following.
   a. Next to the site in the Edit column, select the edit site icon .
   b. Update and save your changes.

   Note: You can't select the same IP Addresses for both the Include and Ignore selections for the Site without triggering an error.

Delete a Site

3. To delete a Site, do the following.
   a. Next to the site in the Delete column, select the delete site icon .
   b. Confirm that you want to permanently delete this site, and select **Delete Site**.

      Note: If devices are associated to a Site, the Site can't be deleted.

Create a Site-specific Variable set

Create a Site-specific Variable for use in Auto Queries. You can use the **Variable** as a credential for your **Site**.

Before you begin
Role required: admin

About this task

Note: A Site can be associated to only one Variable.

Procedure

1. Navigate to the Variable page in the Console.
2. Create a Variable as described in Create a Variable set.
3. Select a Site to associate with the Variable.
4. Create an Auto Query as described in Create an Auto Query.
5. In the Filter section of the query, select the Sites filter.
6. From the list of sites, select the site associated to your variable.
7. Complete creating the query.
8. Run the Auto Query that you created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
Your Site is associated with the Variable and then queried.

Import Sites

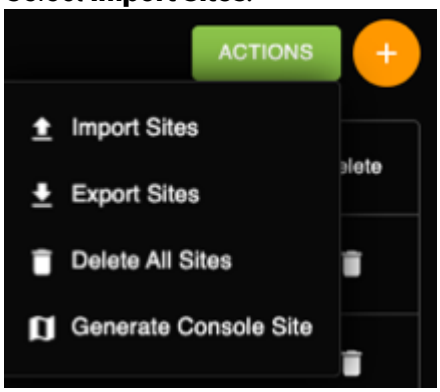
Import existing Sites to the Discovery Console for OT.

Before you begin
Role required: admin

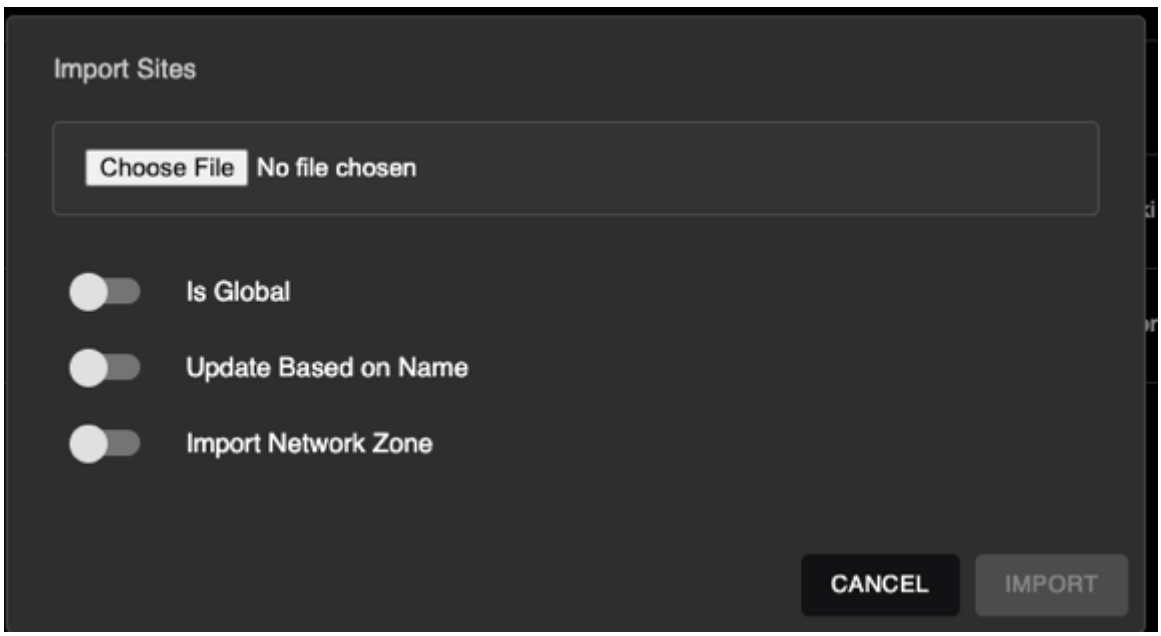
Procedure
1. Navigate to the Sites page.

Import Sites

2. Select the **Actions** button.
3. Select **Import Sites**.



4. In the Import Sites window, choose the type of site and the file that you want to import, and select **Save**.



Export Sites

5. Select the **Actions** button.
6. Select **Export Sites**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
For the exported site, the Sites information is downloaded in the CSV format.

Note: The CVS file includes an Ignored IPs column when applicable to the Site.

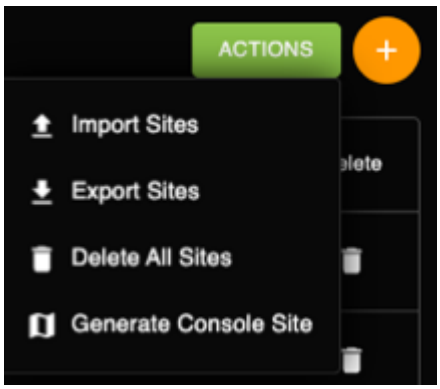
P	Q
NetworkZoneName	IgnoreNetworkZoneName
Nz1	
Nz1	Test NZ1
Nz1	

Export sites

Export Sites on your Discovery Console for OT into a CSV.

Before you begin
Role required: admin

Procedure
1. Navigate to the Sites page.
2. Select the **Actions** button.



3. Select **Export Sites**.

Result
The Sites information is downloaded in the CSV format.

Note: The CVS file includes an Ignored IPs column when applicable to the Site.

P	Q
NetworkZoneName	IgnoreNetworkZoneName
Nz1	
Nz1	Test NZ1
Nz1	

Updates page

The Updates page shows available updates for your Sensor firmware.

The Updates page is organized into the following sections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Deployment

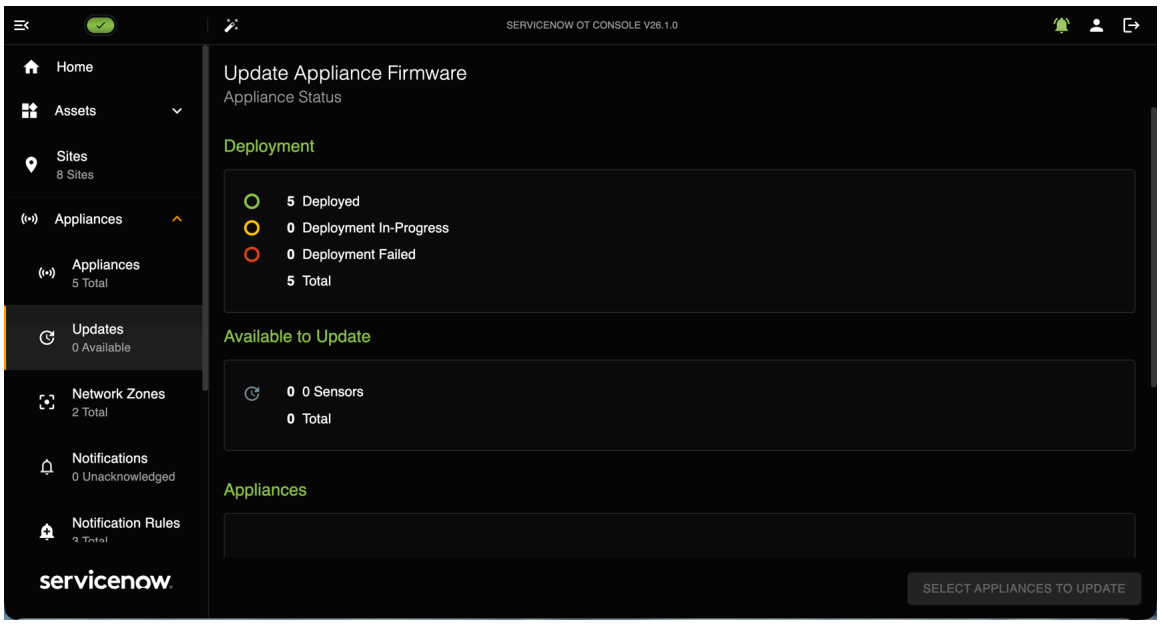
The total number of appliances that are deployed, have deployment-in-progress, or have failed to deploy.

Available to Update

The number of appliances available to update.

Appliances

The appliances that you can select to update. To update the appliance firmware, select the **Select Appliances to Update** button.



Network Zones page

The Network Zones page in the Appliances section includes a list of all Network Zones on the Console. Network zones group assets by IP address to help distinguish one or more assets that share an IP address but are in different local area networks.

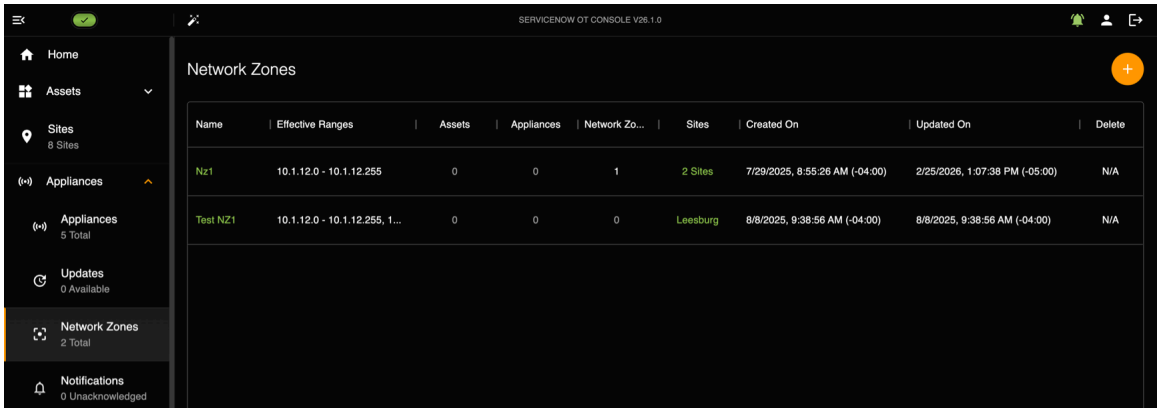
Network Zones group assets by IP address to enable the Console to distinguish one or more assets that share an IP address but are in different local area networks (LANs). For example, due to network address translation (NAT). The Network Zones page includes a list of all Network Zones on the Console along with the following details:

- Effective Ranges for Network Zones operations
- Assets related to the Network Zones
- Appliances related to the Network Zones
- Number of Network Zones
- Created On dates
- Updated On dates

Additionally, each of the Network Zones can be deleted when they are no longer in use. You can select the name of the Network Zones to view them in more detail.

The following image shows an example of the Network Zones page.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Notifications page

The Notifications page shows the notifications available for your Discovery Sensor for Operational Technology (OT).

About this task

You can add a filter to sort and find Notifications related to the following categories.

- End Date
- Rule
- Rule Type
- Severity
- Status

Before you begin

Role required: admin

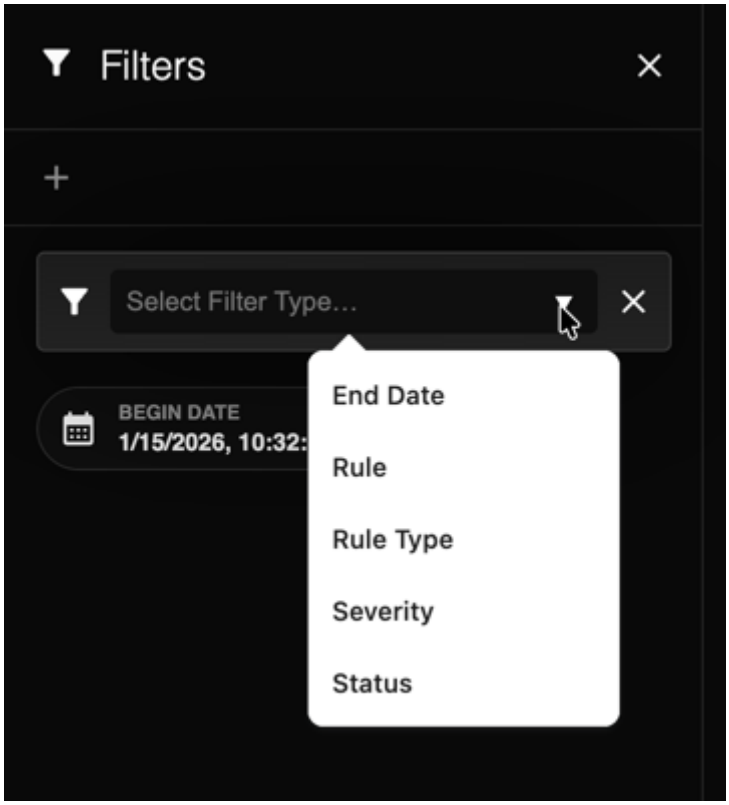
Procedure

1. Navigate to the Notifications page.
2. To filter the notifications, do the following.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the plus icon .
The **Select Filter Type** field opens.

b. Select a filter from the drop-down menu.

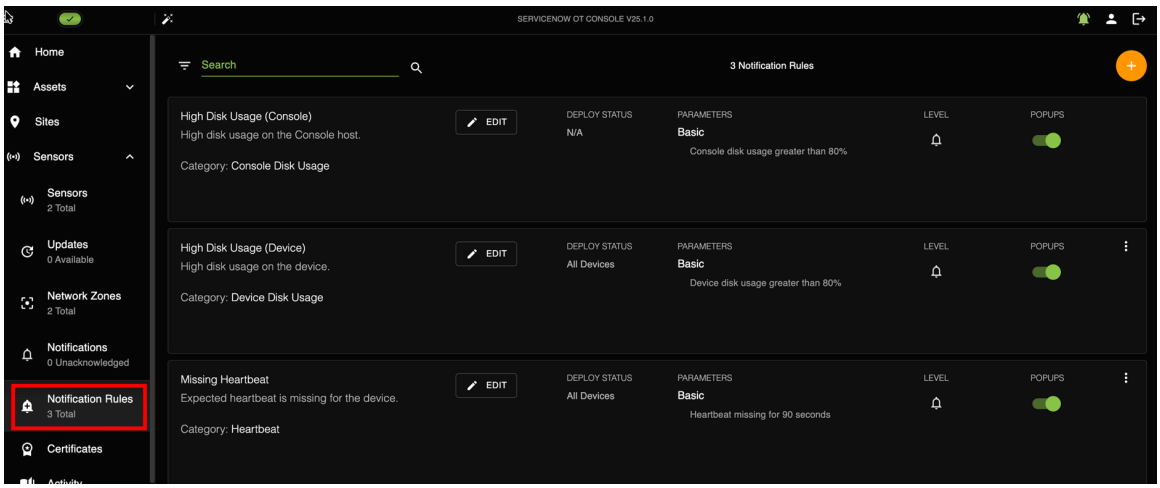


Result

The Notifications are automatically sorted by the selected filter and displayed on the page.

Notification Rules page

The Notification Rules page shows the notification rules that were setup for the Console. Notifications are displayed on the Notification page.



For more information, see Add a Notification rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add a Notification rule

Create a Notification Rule.

Before you begin

Role required: admin

Procedure

1. Navigate to the Notification Rules page in your Console.
2. Select the add icon  .
3. On the form, fill in the following fields.

Notification Rules form

Field	Description
Identification	Name and description for the Notification rule.
Type	Rule type. You can choose from Console Disk Usage, Device Disk Usage, and Heartbeat.
Parameters	Parameters to edit the utilization threshold as needed.
Actions	Add an action for the notification rule from the available list. You can display a message, email, or phone contact. You can also send an email, SMS email, or Syslog. You can add multiple actions to your notification rule.
Notifications	Settings to edit the severity, pop-ups, and suppression of time.

   a. Confirmation
   Confirm your selections in the previous sections.

4. Select **Create Rule**.

Result

The created notification rule displays on the Notifications page.

Certificates page

The Certificates page lets you access data regarding your CA certificates, Sensor credentials, and Collector credentials. You can also renew your certifications from this page.

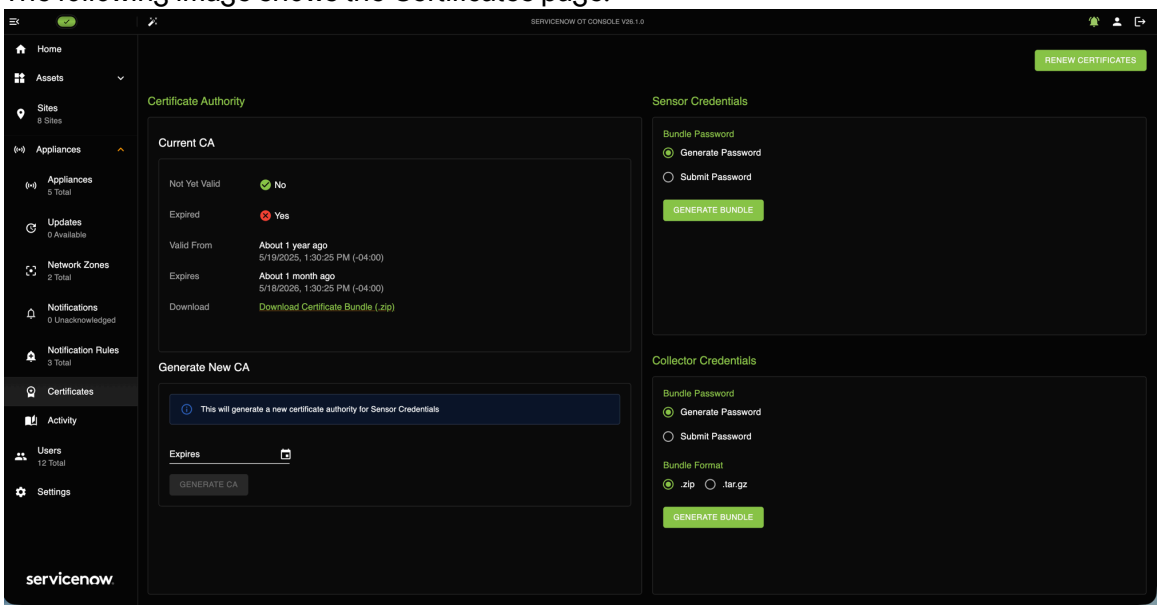
On the Certificate page, you can do the following.

- Generate a Certificate Authority.
- Renew a Certificate.
- Download the Certificate Bundle (.zip).
- Generate a Sensor Bundle using a generated or user-submitted password.
- Generate a Collector Bundle using a generated or user-submitted password. This bundle is generated using the specified bundle format.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For how to renew a certificate, see Renew a certificate.

The following image shows the Certificates page.



Certificate Authority

In the Certificate Authority section, you can generate a new certificate by choosing the expiration date and selecting **Generate CA**.

Select the **Download Certificate Bundle (.zip)** link to download the file containing the Console's Certificate Authority and the server certificate. The certificates establish trust between these applications and confirms their communications are secure and encrypted.

Sensor Credentials

In the Sensor Credentials section, you can generate or submit a password for sensor credentials and then select **Generate Bundle**. The Sensor credentials are formatted in JSON.

Note: The Sensor certificate automatically renews when the Console certificate is renewed.

Collector Credentials

In the Collector Credentials section, you can generate Collector credentials, generate a password bundle, and submit a bundle with either a ZIP file or a tar.gz (tgz) formatted file. Select the ZIP format for Window collectors and the tar.gz format for Linux collectors.

Note: The Collector credentials are formatted in JSON.

When ready, select **Generate Bundle**.

Note: The certificate for the Discovery Console for OT and the Discovery Sensor for OT automatically renews when it is within 30 days of its expiration date.

Renew a certificate

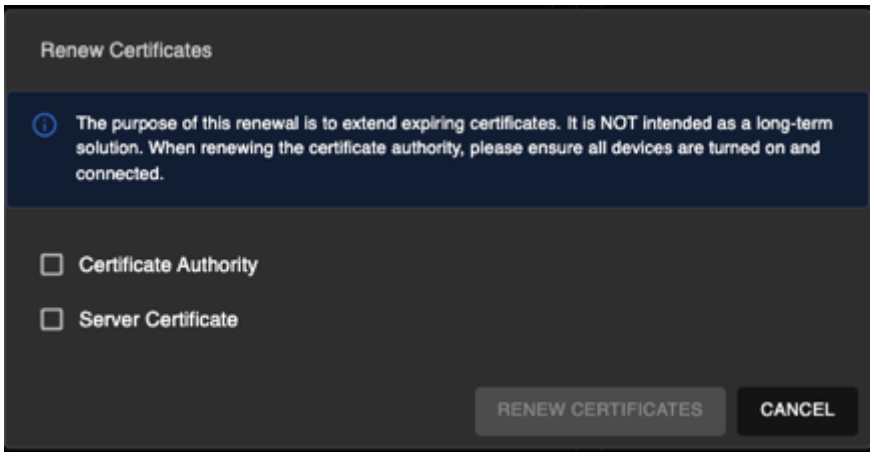
This section describes how to renew a certificate on the Certificates page.

Before you begin
Role required: admin

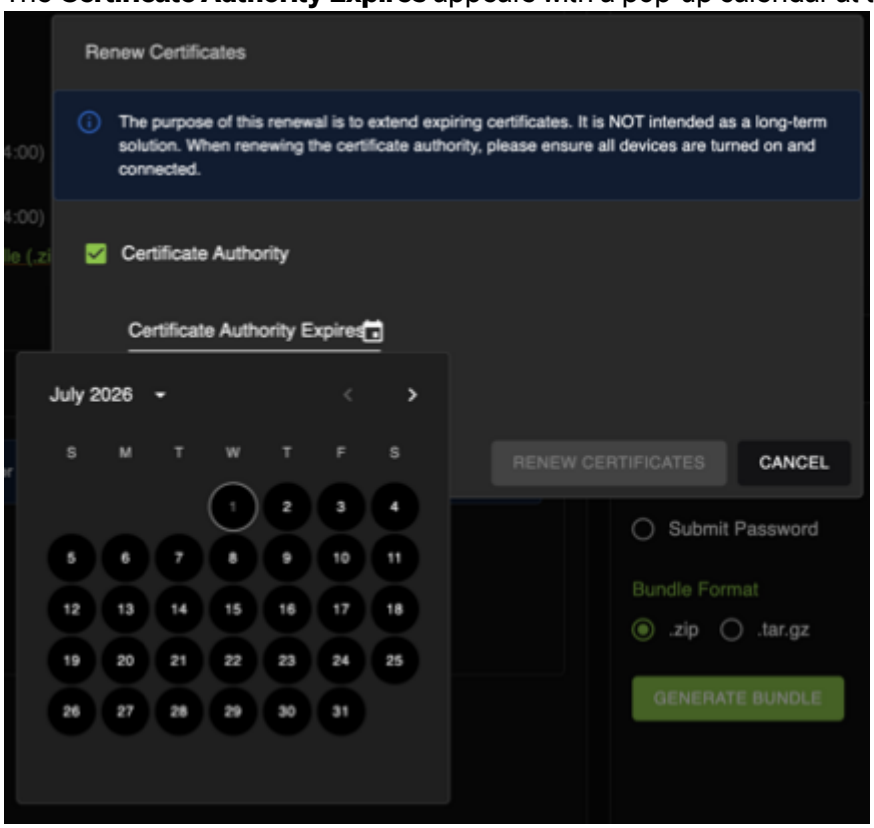
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. From the Certificates page, select the Renew Certificates button.
2. The prompt window opens.
   The prompt reads: The purpose of this renewal is to extend expiring certificates. It is NOT intended as a long-term solution. When renewing the certificate authority, verify all devices are turned on and connected.

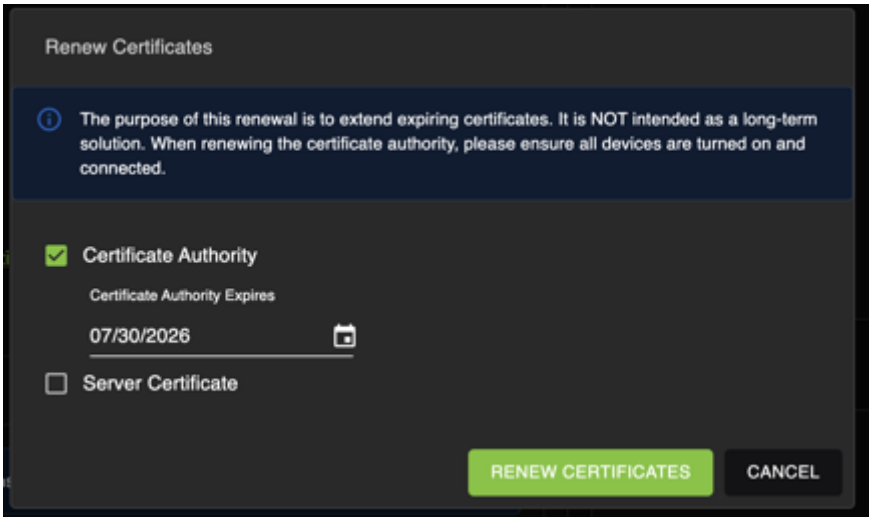


3. Check the box next to either the Certificate Authority or the Server Certificate.
   For this example, the Certificate Authority is chosen.
4. The **Certificate Authority Expires** appears with a pop-up calendar at the end of the line.



5. The calendar opens for you to choose an expiration date.
6. Once you have chosen a date, it appears in the window after the Certificate Authority.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Note: This renewal does not generate a new private key pair. The Console keeps track of old and the new certificates. To avoid issues, renew the Sensors and Collectors certificates at the same time. Renew all certificates at least 48 hours before the expiration date and verify that all devices are online to verify the automated retrieval occurs. After they are retrieved, there is a small interruption as the Sensor and Collectors restart to load the new certificates.

Activity page

The Activity page lists only the Appliance activity on your system.

Your Appliance activity is organized by the most recent activity and shows the date and time the activity took place. The page also displays the Appliance name, the type and subtype of activity, and any additional details.

Users page

The Users page shows the lists of both active and inactive users in your Discovery Console for OT system. You can access the Discovery Console for OT through user accounts available in the system.

User overview

The following user accounts are available in the system.

- Administrator accounts, which have full access to the Discovery Console for OT's functionality and features
- Non-administrator accounts, which have limited access to the Discovery Console for OT

Note: Each user who needs access to the console is given a user account with private credentials. The Console application records user activity in the system. Sharing accounts or account passwords prevents an accurate audit of system activity.

Registering the initial user

When the Discovery Console for OT is accessed for the first time after installation, the console guides the operator through the initial user registration process. The initial user account is created as an administrator account and has access to all features of the application.

The following sections describe how to create and register the initial user.

Step 1: Accepting the End User License Agreement

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You must read and accept the End-User License Agreement (EULA) before you can set up the initial user. Confirm that an individual with legal authority and authorization has also reviewed the EULA before accepting the agreement.

Step 2: Creating the Initial User

After you accept the EULA, you're prompted to register the initial user. A username, password, and email address are required to complete the account setup. You must complete all of the fields before you can register the user.

The initial user is automatically assigned the administrator role and has full access to the system. Save the password for the initial user account in a secure place. The administrator account is necessary to create accounts for additional users.

Note: If all administrator accounts are inaccessible, contact your Discovery Console for OT representative for assistance.

Managing user accounts

On the Users page, you can view all of the users in the system. Administrators are the only users that can list, create, or view information and update another user's information in the system. Administrators can also force a user to change their password on their next log in.

To view a user's information, you can select the user on the Users page.

User roles

When creating user accounts, you can assign the following roles.

Note: You can assign more than one role to a user.

Discovery Console for OT roles

Role	Description
Admin	Can access the full functionality of the Discovery Console for OT. Can create, edit, and remove user accounts.
Reader	Can view the Discovery Console for OT with read-only permissions.
User	Can access the Discovery Console for OT with limited permissions.

Note: For more information, see Set up a Microsoft Entra ID next.

Set up a Microsoft Entra ID

This section describes how a Discovery Console for OT user can set up an **Microsoft Entra ID** integration.

Before you begin

Role required: admin

About this task

The **Microsoft Entra ID** integration enables users to log in to the Discovery Console for OT using their organization's **Microsoft Entra ID** cloud identity access management (IAM) credentials. This removes the need for managing separate usernames and passwords within the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This feature relies on configuring an application in **Microsoft Entra ID** and providing the required details in the Console settings.

Note: This feature requires the Discovery Console for OT to have internet access.

This integration allows seamless and secure authentication using **Microsoft Entra ID**, improving user experience and aligning with enterprise identity management practices.

To enable an **Entra ID** log in, an administrator must complete the following steps.

Note: Check with Microsoft for the latest documentation before you begin this procedure.

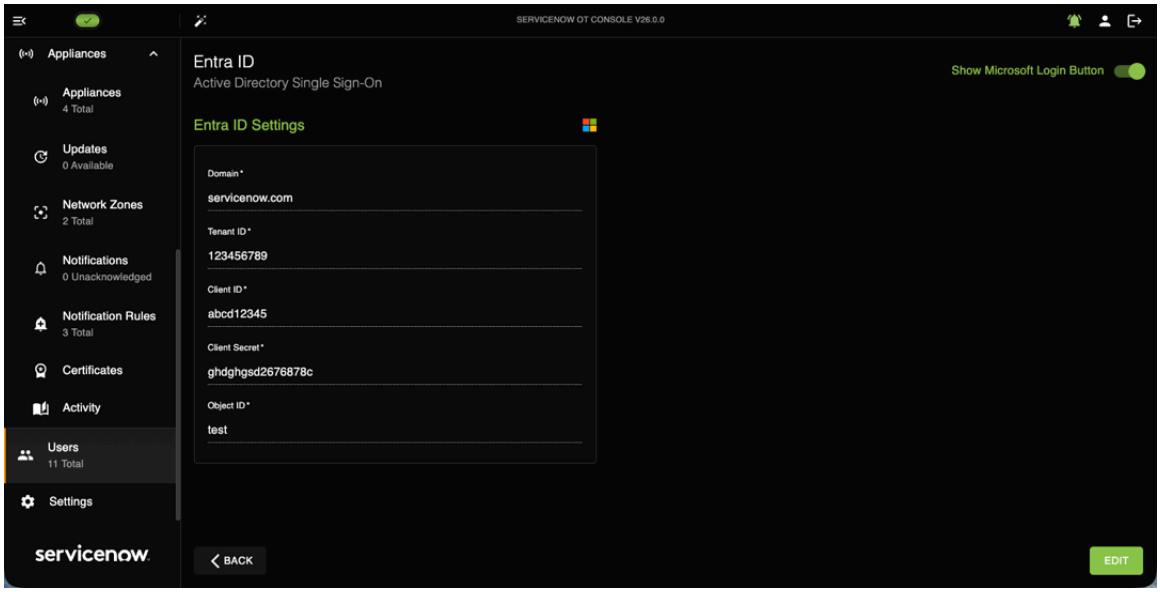
Procedure

1. Register an application in Entra ID.
2. In the Azure application:
   a. Navigate to **Entra ID > App** registrations.
   b. Create a new application; for example "Console app".
   c. Configure a Redirect URI pointing to the Console URL; for example, https://<console-url>.
3. Collect required values.
   From the Entra ID application, locate the following information.
   - Domain: Organization's primary domain, for example, company.onmicrosoft.com.
   - Tenant ID: Found in the Entra ID **Overview**.
   - Client ID: Application (client) ID from App registration.
   - Client Secret: Generated under **Certificates & secrets**.
   - Object ID: Application object ID.
4. Configure Console settings.
5. In the Discovery Console for OT:
   a. Navigate to **Console > Users**.
   b. Next to the **Actions** button, select **Settings**.



   c. Enter all required values.
      - Domain
      - Tenant ID
      - Client ID
      - Client Secret
      - Object ID

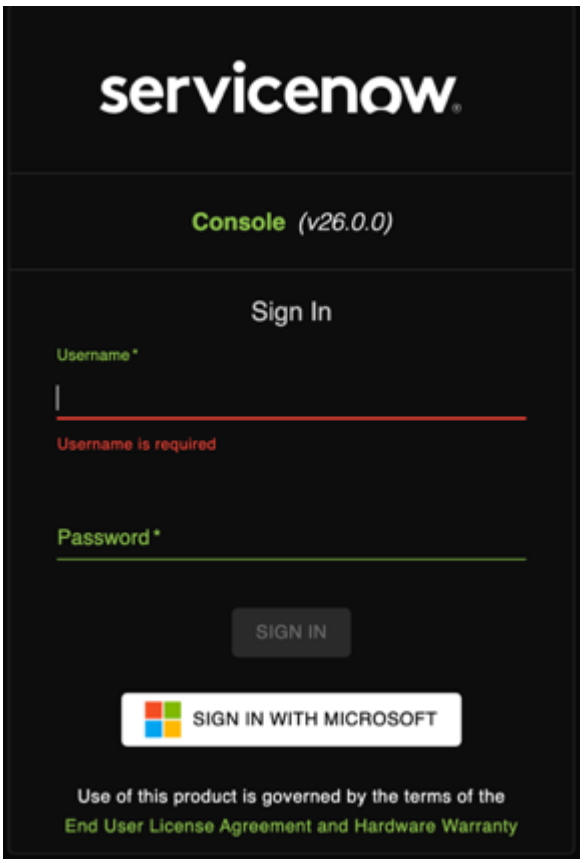
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



d. Select **Save**.

6. Enable the log in option.

- In the Entra settings, toggle **Show Microsoft Log in button**.
- This enables the SSO log in for end users.



Result
Once configured, user can log in by doing:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Open the Console log in page.
2. Select the **Sign in with Microsoft** button.
3. Authenticate using the organization's Microsoft account.
4. After successfully authenticating, the user is redirected to the Console and is logged in.

Note: Important considerations:

- The Client secret must be kept secure and renewed before expiration.
- The redirect URI in Entra must exactly match the Console URL.
- Incorrect Tenant ID or Client ID results in authentication failures.
- Admin consent may be required when configuring permissions in Entra.

Create a user

Create a user account that can access the Discovery Console for OT.

Before you begin

Role required: user

Procedure

1. Navigate to the Users page.
2. Select the add icon  .
3. On the form, fill in the following fields.

Add user form

Field	Description
Username	Username for the user account.
Email	Email for the user's account.
Password	Secure password for the user account.
Confirm Password	Retype the password.
Roles	Roles that the user account needs. If needed, you can select more than one role.

Edit a user's information

Edit a User's information and keep the user account up to date.

Before you begin

Role required: admin

Procedure

1. Navigate to the Users page.
2. Select the user account that you want to modify.
3. Select **Edit**.
4. Edit the available fields as needed.
5. Select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Force a password reset

Force a user to reset their password.

Before you begin
Role required: admin

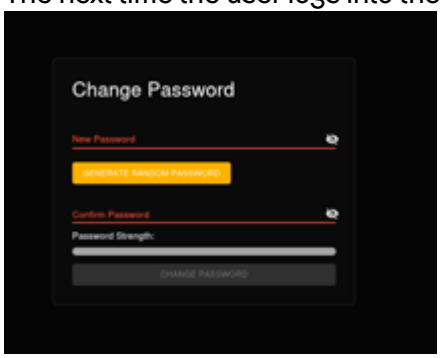
About this task
An administrator can force another user to change their password the next time that user logs on to the Console.

Procedure

1. In the Console, navigate to the Users page.
2. You can force a user to change their password by clicking on the green key.
3. Refresh the page.
   The green key changes color to an orange key with backwards slash through it. This means the user needs to change their password the next time they log in. The key image does not display once the user changes their password and logs back in.



   The next time the user logs into the console, the **Change Password** window opens.



4. Enter a new password and then enter it again to confirm it.
   For guidance, the Change Password window displays the Password Strength.
5. Select **Change Password**.

Deactivate a user

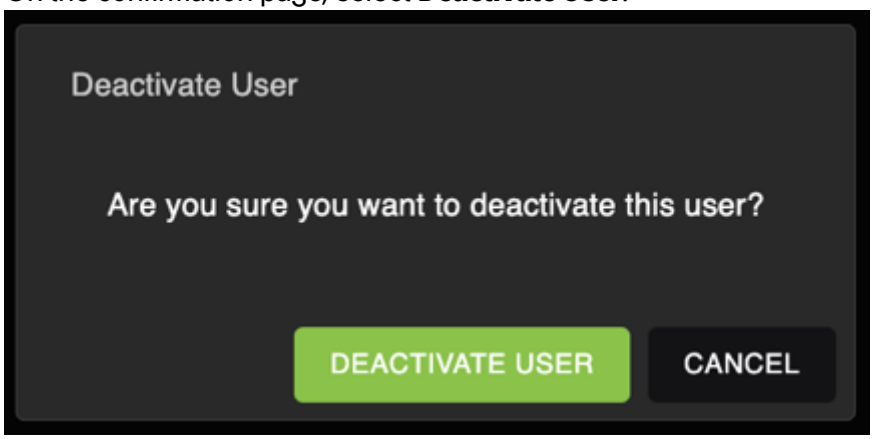
Deactivating a user verifies that they can't access the Discovery Console for OT.

Before you begin
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to the Users page.
2. Next to the user you want to deactivate, select the Deactivate User icon .
3. On the confirmation page, select **Deactivate User**.



Settings page

The **Settings** page lets you view and modify system-wide settings for the Discovery Console for OT, Discovery Sensor for OT, and the OT Discovery Collector.

Settings page overview

To open the Settings page, select **Settings** from the main navigation menu. The Settings page is divided into tabs and opens to the **Console** tab view. The Settings page is organized by the following tab configuration options.

Console

The Console tab on the main Settings page is divided into the following sections.

- **About**

  The Console tab includes a link to the End-User License Agreement (EULA), the version number of the Console, and the Console ID.

- **License**

  When you first sign into the Console, a warning banner alerts that you need a license. When you use the interactive configuration wizard, you're also alerted to the license status. For more information, see Requirements for Discovery Console for OT installation.

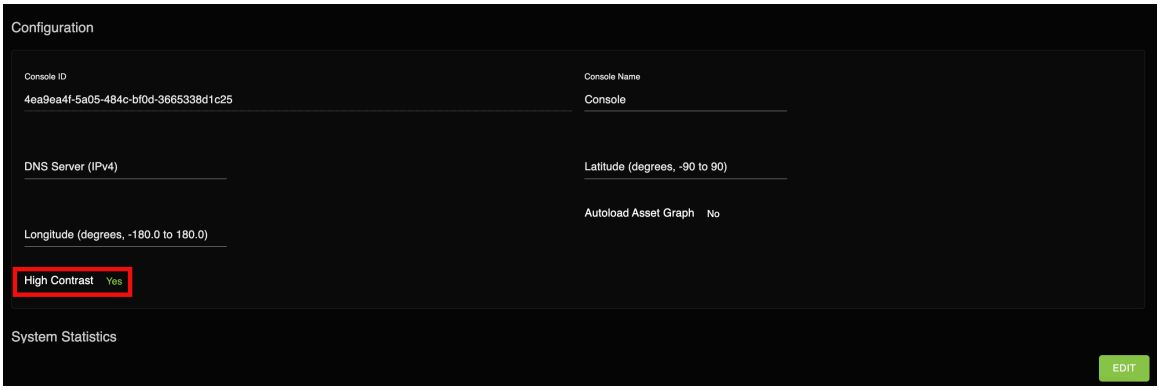
  Note: If needed, request a Console license from your ServiceNow account representative.

- **Configuration**

  The Configuration section displays the Console Name of the local web Console. The Console Name is used in Syslog messages.

  In the Configuration section, use the **High Contrast** setting to change hyperlinks from orange to green for ease in viewing. To change this setting, select the **Edit** button, then slide the **High Contrast** toggle to **Yes**. Select **Save** to save your changes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



- **System Statistics**

  The Console settings show disk and memory usage for its host server. It's important to maintain an adequate disk and memory space so that the Console continues operating properly. Check the system statistics periodically to confirm that proper resources are available.

Certificate

On the Certificate tab, you can check the Console Certificate status. You can also update the certificate by selecting Generate New Bundle or Upload Bundle (.p12) and then selecting the **Generate Bundle** button.

Note: The Certificate tab does not function the same as the **Certificates** page.

API

The API settings manage active and denied tokens and provide endpoint configuration files for the Service Graph Connector for ServiceNow OT Discovery.

Email

The Discovery Console for OT can be configured to send email and SMS text alerts when certain conditions occur within the system. To do so, the Console relies on an external mail server to send messages.

In the Email Server Configuration panel, enter the settings that match your mail server configuration. The Discovery Console for OT uses these settings whenever the **Enable Alert Notifications** setting is activated.

Exports

The Export tab downloads data from the Console to JSON files. Available data types include Assets, Sites, Software, Sensors, Network Zones, Notifications, Images, and All. Selecting All bundles and downloads data from all categories in one ZIP file.

Metadata

The Metadata tab includes settings for several features related to metadata that can be used to enrich the analysis and reporting of data collected by the Console. For example, you can set up metadata to provide more details about the connections observed in the network.

The following table describes the different sections of the Metadata tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Section	Description
CVE Database Package	Enables you to import a CVE package. You can use the **Import CVE Package** button to import a package locally saved on your computer. **Note:** You can obtain a current CVE database file from your ServiceNowOperational Technology Discovery representative.
Query Driver	Enables you to import or download query drivers and set the concurrence and speed of Sensor and Scout queries. You can use the **Import Query Driver** button to import a query driver from your computer or **Download Query Driver** to download the current query driver and save locally. To edit the Query Driver settings, select the **Edit Settings** button.
Common Port Names	Defines a mapping between port numbers and protocol names. This information is used in the Console to display protocol names when you create a ports activity report. This feature must be turned off to import a new port name file. To enable or disable this setting, select the **Edit** button under the Common Port Names and Ethernet vendor sections. A current port names file can be obtained from your Discovery Console for OT representative.
Ethernet vendors	Defines a mapping between MAC addresses and vendor information. This information is used in the Console to provide vendor information for assets. This feature must be turned off to import a new Ethernet vendors file. To enable or disable this setting, select the **Edit** button under the Common Port Names and Ethernet vendor sections. A current Ethernet vendors file can be obtained from your Discovery Console for OT representative.

Package

In the Package tab, you can use the package source options under the **Package Manager Configuration** section. You can import packages by file upload or from a remote repository.

Note: The package manager must be configured so that your Discovery Console for OT sensors can receive firmware updates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reprocess

The Reprocess feature allows the system to reevaluate previously collected Auto Query scan results using the latest query driver logic. See Reprocess Auto Query results for more information.

Syslog

In the Syslog tab, you can configure a Syslog server. After configuring these settings, Syslog data can be forwarded from the Discovery Console for OT to a separate Syslog data consumer. For example, the Splunk enterprise security data analysis tool set.

Logs

From the Logs tab, you can download Discovery Console for OT logs. You have the option to choose whether to download logs on the current day, on a custom date, or on a date range.

For more information, see Download Console log files.

Certificate tab

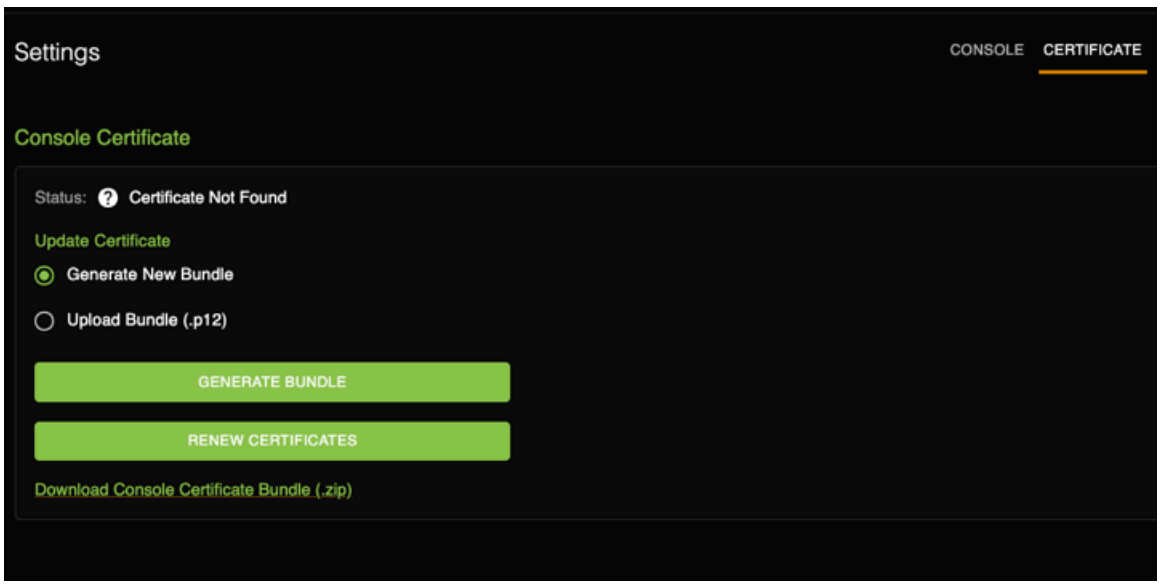
The Certificate tab is for generating or uploading the Discovery Console for OT certificate.

Console Certificate

The Console generates its own self-signed certificate bundle when initially deployed. The Certificate tab is for updating, generating, uploading, or downloading a Console Certificate.

On the Certificate tab you can select from the following actions to update a Console Certificate:

- Generate New Bundle.
- Upload Bundle (p12).
- Download the Certificate Bundle (.zip).
- Renew Certificates.



After you generate a New Bundle, you can select the link **Download Console Certificate Bundle (.zip)**. The bundle contains the Console's Collector Certificate Authority and the RabbitMQ certificate. These certificates establish trust between the Console and Collector and confirms their communications are secure and encrypted.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For more information, see Renew a certificate. The steps are similar but the Certificate tab only pertains to the Console Certificate.

Discovery Console for OT API

You can access the Console Discovery data via the API. On the Settings page, select the **API** tab to view and use the active tokens, denied tokens, and endpoints needed to communicate with the Service Graph Connector (SGC).

Note: To learn more about the Service Graph Connector, see Service Graph Connector for ServiceNow Operational Technology (OT) Discovery

API settings

The API settings are used to set up the active tokens, denied tokens, and endpoints needed to communicate with the SGC for ServiceNow Discovery for Operational Technology (OT).

Tokens can be imported or exported, and endpoints can be downloaded.

The SGC enables the API to communicate data from the Discovery Console for OT and other Discovery components to the ServiceNow instance. Data can also be communicated to and from external APIs.

Functionality

The SGC has been enhanced for better connection to and from the Discovery components, the Discovery Console for OT API, and your ServiceNow instance.

The SGC provides Discovery Console for OT API functions such as:

- Sends the status of the user license.
- Imports all software programs that are identified on the devices and returns a paginated list from the SoftwaresAPI view.

  The API ingests software and provides the following program attributes:

  - `inputProduct`: the software name
  - `Version`: the version of the installed software
  - `inputVendor`: the manufacturer of the software
  - `lastSeenOn`: the assets' LastSeenOn field added to the object
  - `assetId`: derived fro the _id for the asset document containing the software array.
  - `_id`: for the document; should be the _id for the object in the software array
- Transfers images and screen shots from the Console to the ServiceNow instance. This returns images in a paginated list with these filters:
  - `UpdateOn`
  - `CreatedOn`
  - `ScreenShot`
  - `Size`
  - `OCR Words`
  - `Titles`
- Pushes Discovery Sensor for OT information to the ServiceNow instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The API can be used to return the `sensorId`.
- You can gather information about the Sensor and use it to discover assets.
- Sensor information can be pushed via the API to the ServiceNow.

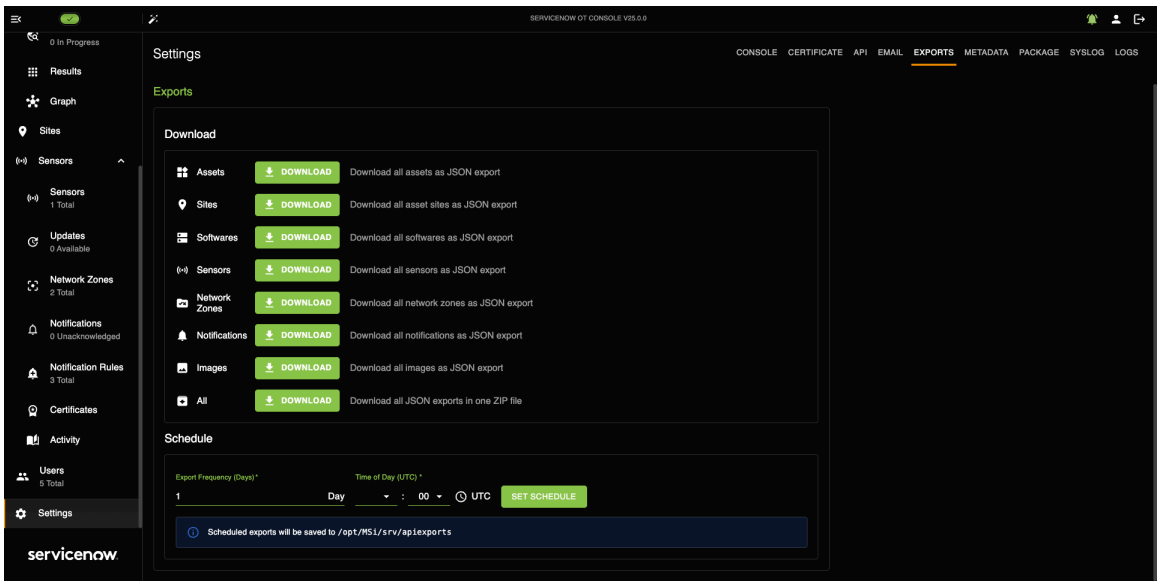
- Send to the Console virtual machine (VM) health metrics and host metrics of the Sensor and the Scout. This helps with visibility of version, installed processes, and the health of the host machine of Discovery Console for OT, Discovery Sensor for OT, and Discovery Scout for OT.

Indirect network connection (air-gapped)

For security reasons, a computer or system may not be directly connected to the internet or may be on an unsecured LAN. In such a situation, the Discovery for Operational Technology components cannot push files or data to the MID Server and from there via the Service Graph Connector on to the ServiceNow instance.

To solve the air-gap issue, the Discovery Console for OT can generate JSON files. These JSON files are physical files and can be manually copied and then moved to the MID server via an external drive. They can then be manually copied to a specific directory on the MID server and then consumed through the SGC to the ServiceNow instance.

For example, if you navigate to **Settings > Exports** on the Discovery Console for OT, you can download data generated by the Discovery components as a JSON export file. You can schedule the frequency of these downloads setting the number of days and time of day. These files are saved to the `/opt/MSi/srv/apiexports` directory. From there you can move them to physical media like a thumb drive. You can then copy or import the JSON files to the MID Server and on to the SGC and then to the ServiceNow instance.



To edit the Console API, see Edit API settings.

Edit API settings

Edit the API settings for the Discovery Console for OT to generate active tokens, remove denied tokens, or view the available API endpoints needed to communicate with the Service Graph Connector (SGC).

Before you begin
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The Service Graph Connector (SGC) has been enhanced to enable functions of the Discovery Console for OT API.

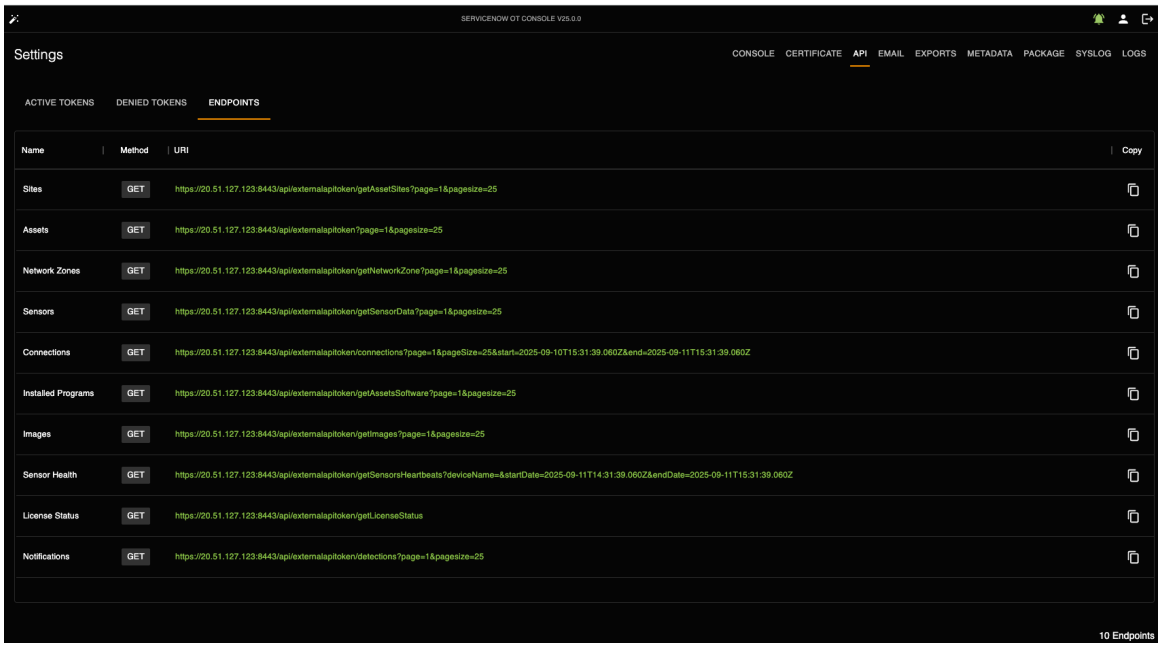
Procedure

1. In the Console, navigate to the **Settings** page.
2. On the Settings page, select the **API** tab.

Active Tokens

3. Generate an API token.
   a. Select the **Active Tokens** tab.
   b. Select the add icon  .
   c. In the Generate API Token window, select the expiration date.
   d. Select **Generate Token**.
4. Remove denied tokens.
   a. Select the **Denied Tokens** tab.
   b. Next to the API token that you want to remove, select the **Remove Token**  icon.
5. View the available **Endpoints**.
   The endpoints are listed in columns by name, method, and their URI. The following endpoints are available for the Discovery Console for OT.
   - **Sites**
   - **Assets**: Returns the `DeviceId` for each asset; if no `DeviceId` is set, then it returns `null`.
   - **Network Zones**: Returns values for the Network zone, parent/child zones, subnet information, and IP ranges.
   - **Sensors**: Returns the Sensor id (`sensorId`) that points to the sensor that was used for the discovery.
   - **Connections**
   - **Installed Programs**
   - **Images**
   - **Sensor Health**
   - **License Status**: Returns the status of the license and whether it is expired, to the Discovery Console for OT.
   - **Notifications**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



a. Select the **Endpoints** tab.

b. Select the copy icon ( ) to copy the endpoint.

c. The data is matched to the API.

d. Automatically store files under `./apiexports`.

e. Use the naming convention `${API}_${DATE}.json` (for example, `Assets_19791231.json`).

f. After creating the new file, delete any previously created files.

g. Only generate files if there is sufficient disk space.
The disk space available is limited to 1 GiB.

Edit email settings

Edit the email settings as needed to match the settings on your mail server.

Before you begin

Role required: admin

Procedure

1. Navigate to the Settings page.
2. Select the **Email** tab.
3. Select **Edit**.
4. On the Email Server Configuration form, edit the following fields as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Email Server Configuration

Field	Description
Host	IP address of the email server.
Port	Port of the email server. Typically port 25.
From Address	From address to use for the alert
Enable TLS Encryption	Setting that must match the TLS setting on the email server.
Enable Connection Logging	Option to log all email server connections to a file

5. Select **Save**.

Export data

The Discovery Console for OT exports data as a JSON export file.

Before you begin

Role required: admin

Procedure

1. In the main menu, select the **Settings** option.
2. On the Settings page, select the **Exports** tab.
3. Select and export data into JSON files.
   The available data includes the following.
   - Assets
   - Sites
   - Softwares
   - Sensors
   - Network Zones
   - Notifications
   - Images
   - All

   Note: Selecting **All** downloads all JSON exports to one zip file.
4. Select the **Download** button next to the desired data.
5. Under the **Schedule** heading, select the export frequency by number of days and time of day (UTC).
   The default frequency is 1 day. The time-of-day defaults to 00:00 AM UTC.

Result

The scheduled exports are saved to `/apiexports`.

Create a backup for the Console

You can create a full or partial backup of the Discovery Console for OT data.

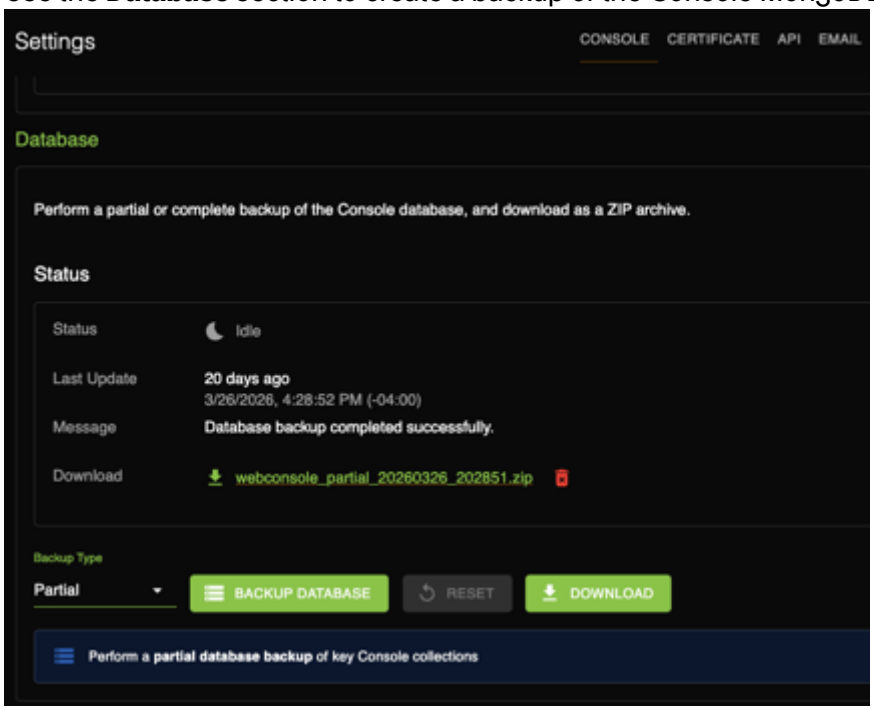
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
To create a backup for the Console, you must have **admin** access.

To support disaster recovery, the Discovery Console for OT generates backup files containing restore data, configuration, and logs. Console administrators can initiate backups and restore the Discovery Console for OT, the Discovery Sensor for OT, and the OT Discovery Collector to their previous states when needed. This enhancement provides reliable disaster recovery capabilities across all system components.

Procedure
1. Navigate to **Settings > Export** tab.
2. Use the **Database** section to create a backup of the Console MongoDB.



3. Select the **Backup Type** and select from the drop-down menu.
   - A **Full** back up includes:
     - entire WebConsole database
     - all images
   - A **Partial** backup only includes the collections defined in the `PartialIncludeCollections` setting in `appsettings.json`.
4. If you select a **Partial**, the downloaded ZIP file, by default, includes only the following collections.
   - AssetAutoScans
   - AssetDeviceMessages
   - AssetDeviceStatistics
   - AssetDevices
   - AssetProperties

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- AssetRevisions
- AssetScanResults
- AssetScanResultsArchive
- AssetScans
- AssetSites
- Assets
- CyberDashboards
- DetectionRules
- DetectionScoreDetails
- Detections
- DeviceErrors
- DevicePolicyStatus
- DeviceScoreDetails
- DeviceWhitelistApplicationPermissions
- Devices
- EthernetVendorOrganizations
- EthernetVendorRanges
- EthernetVendors
- ExternalAssets
- NetworkZones
- Settings
- UnsafePorts

Image files aren't included in a Partial backup.

5. Archive data can be included or excluded based on the system configuration.
6. You can set system configurations during the Console installation process.
7. The backup behavior for archived query results is controlled by the following Backup configuration settings in the `appsettings.json` file.
   - If `ExcludeArchiveFromFull` is set to **true**, archived scan results are excluded from the Full backup.
   - If `ExcludeArchiveFromFull` is set to **false**, archived scan results are included in the Full backup.
   - If `ExcludeArchiveFromPartial` is set to **true**, archived scan results are excluded from the Partial backup.
   - If `ExcludeArchiveFromPartial` is set to **false**, archived scan results are included in the Partial backup, provided that `AssetScanResultsArchive` is listed in `PartialIncludeCollections`.

   a. Full backup

   - If `ExcludeArchiveFromFull = true` Archive **NOT included**
   - If `ExcludeArchiveFromFull = false` Archive **INCLUDED**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. Partial backup

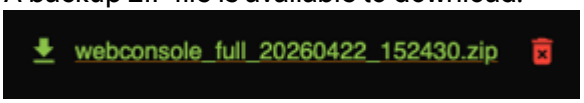
Even though `AssetScanResultsArchive` is in your list for backup in configuration:

- If `ExcludeArchiveFromPartial = true` Archive **NOT included**
- If `ExcludeArchiveFromPartial = false` Archive **INCLUDED**

8. After deciding the **Backup Type**, select the **Backup Database** button.



9. When the backup is finished, the screen displays "Database backup completed successfully."
10. A backup ZIP file is available to download.



11. Select the **Download** button and the ZIP is downloaded to your local system.
12. Once the file is downloaded, select the delete icon (trash can) to remove the archive and free up disk space on the Console.

Edit the Query Driver on Metadata tab

Edit the Query Driver on **Metadata** tab. The Query Driver section enables you to import or download query drivers as well as control the speed of Auto Queries.

Before you begin

Role required: admin

About this task

The **Metadata** tab includes settings for several features related to metadata that enhance analysis and reporting in the Discovery Console for OT. The **Query Driver** settings control your Sensors' performance and resource usage. These settings manage how quickly Auto Queries are executed and how much load is placed on your network devices. They also regulate how many queries a Sensor can execute simultaneously. The **Delay** setting specifies the interval between consecutive queries. For example, setting the delay to 50% effectively halves the time between queries and operating the query at a faster pace.

Procedure

1. Navigate to the **Settings > Metadata** tab.
2. In the Query Driver section, you can import or download the Query Driver.
3. To edit the Query Driver, select the **Edit Settings** button.
   The **Query Driver Settings** window opens.
4. In the Sensor Load section of the window, use the sliding scale to change settings for the Query Load and the Discovery Load.
5. In the Delay section of the window, use the sliding scale to change the Query Delay settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



6. Select the **Save Settings** button to save, or the **Cancel** button to discard your changes.

Upload firmware packages

If you're using a local repository, upload firmware packages to the Discovery Console for OT so the system knows when an update is needed.

Before you begin

Role required: admin

Procedure

1. Obtain the latest firmware packages directly from your Discovery Console for OT account representative.
2. Navigate to the Settings page and open the **Package** tab.
3. Select **Import Packages**.
4. Select the provided firmware package and select **Open** to upload the files.
   The Package Import status modal window tracks the upload status.
5. Repeat steps 2–4 for each firmware package.

Result

The Discovery Console for OT verifies the integrity and authenticity of the uploaded file before they're made available for device updates. Packages that fail authenticity checks are automatically rejected during the upload process.

Reprocess Auto Query results

On the Settings page, the Reprocess tab is available to reprocess Auto Query results.

Reprocess feature

The Reprocess feature allows the system to reevaluate previously collected Auto Query scan results using the latest query driver logic. This is useful when a query driver(s) is updated. Instead of rescanning devices, the system reuses existing stored scan results and processes them again. The results display on the Results page.

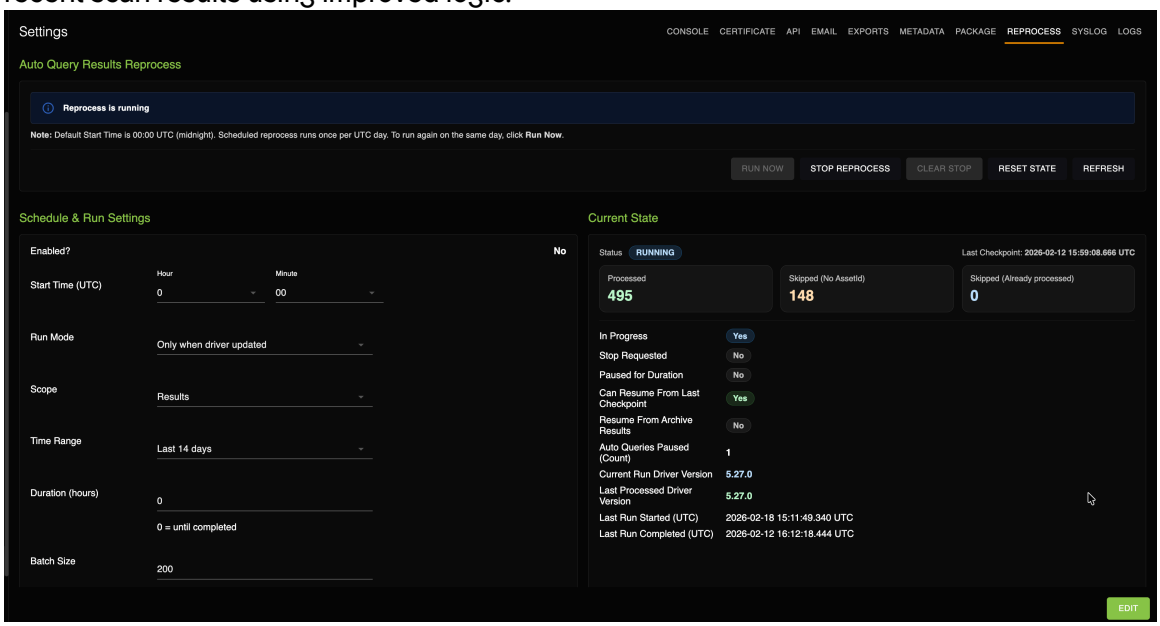
The Reprocess feature runs based on the configured schedule. As displayed in this table, you can schedule your configuration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configurations

Setting	Options
Start time	Default: 12:00 a.m. UTC
Run Mode	• Always • Only when the Query Driver version changes (default setting)
Scope	• Results only • Results + Archived Results
Time range	Last 17 days, Last 30 days, or Custom. Default is the last 14 days.
Duration	Until completed or time-limited
Batch size	No default.
Enable?	Yes / No

After upgrading to a new query driver version, enable the Reprocess schedule to reevaluate recent scan results using improved logic.



Edit Syslog settings

Edit the Syslog settings as needed to configure the Syslog server.

Before you begin

Role required: admin

Procedure

1. Navigate to the Settings page.
2. Open the **Syslog** tab.
3. Select **Edit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. On the form, edit the following fields as needed.

Email server settings

Field	Description
Host	IP address of the Syslog host
Port	Port that the host listens on. Typically port 514 for Syslog.
Transport	Transport protocol used by the host. Typically, UDP.
Facility	Descriptor used to indicate which process on the machine created for the Syslog event.
Level	Desired Syslog severity level that's pushed to the receiving server.
Audit Log Messages	If toggled on, enable Audit Log Messages.

5. Select **Save**.

> **Important:** Be sure to adjust any network firewall rules to open the specified Syslog port and protocol. Otherwise, traffic from the Discovery Console for OT can't reach the receiver application.

Download Console log files

The Console logs are available to download for tracking or troubleshooting purposes.

Log files

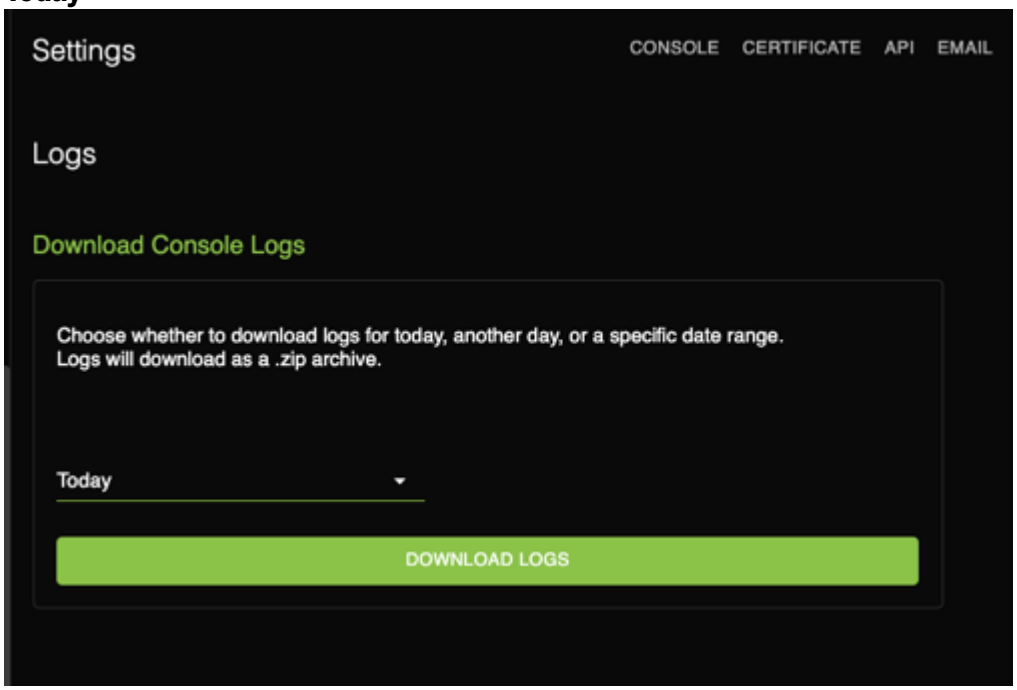
You can download log files for the Discovery Console for OT.

To download these logs, do the following.

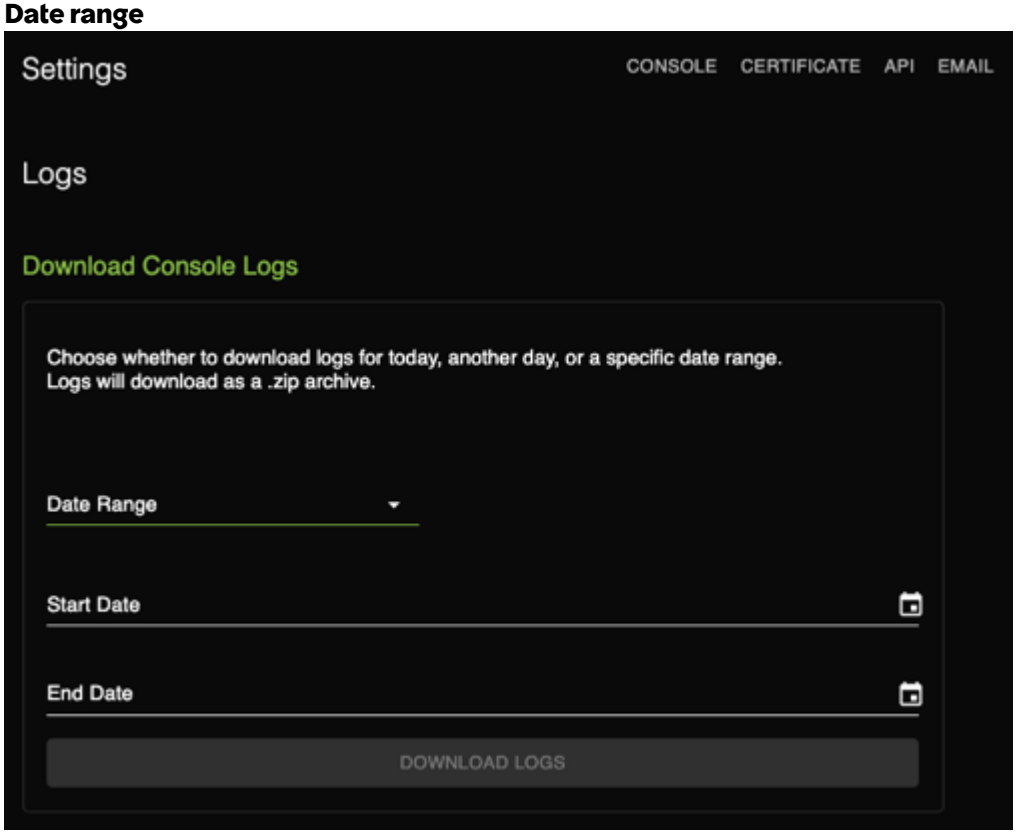
- In the Console, go to the Settings page.
- On the Settings page, select the **Log** tab.
- In the drop-down field, select one of the date settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Today**

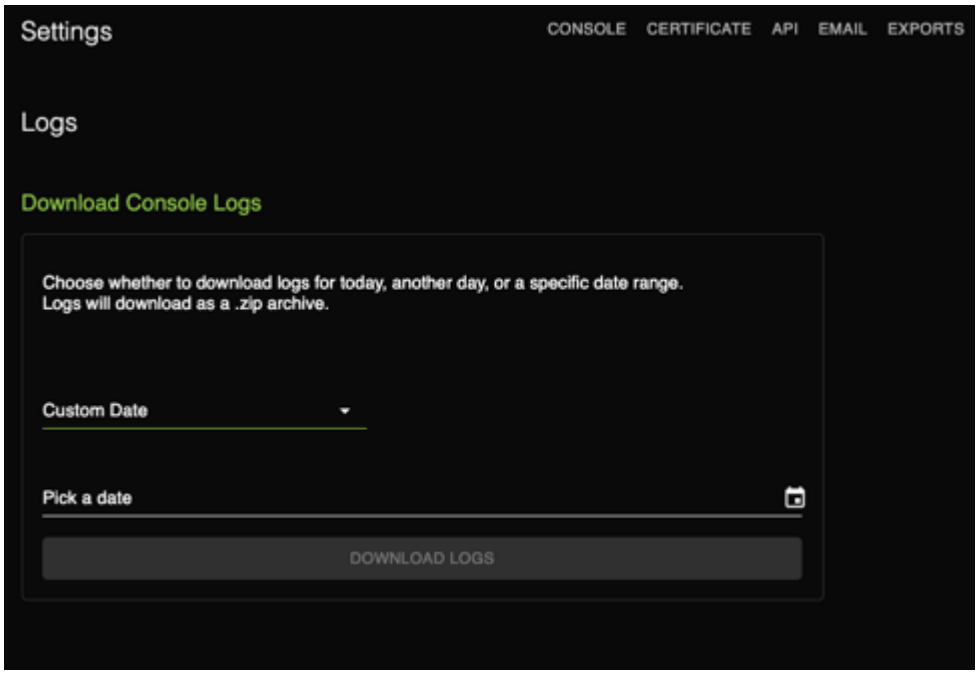


- **Date range**



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Custom date**



- Select **Download Logs** to download a compressed zip file of all log files.

Sensor log files

The Console has an early access capability for retrieving Sensor logs. Currently, accessing these logs requires deep technical expertise of the system. Leave this feature inactive unless directed to enable from Customer Service and Support.

If you have questions or need assistance, contact Customer Service and Support.

Discovery Sensor for Operational Technology (OT)

Use the Discovery Sensor for Operational Technology (OT) application to discover and query devices in the Operational Technology environment.

Get started

Use the links in the Related Topics section to explore, configure, and learn more about the ServiceNow Discovery Sensor for Operational Technology (OT).

Log files

To review files on your Sensor and access logs for troubleshooting purposes, you can SSH from another machine that has network access to the Sensor. If you have to authenticate, use the default credentials. Refer to Configure the Discovery Sensor for OT for the credentials.

Explore the Discovery Sensor for Operational Technology (OT)

The Discovery Sensor for OT provides you with enhanced scanning and query functionality to manage your assets in the OT environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Discovery Sensor for OT overview

This section provides an overview of the Discovery Sensor for OT and its integration with the Discovery Console for OT. For more information, see Discovery Console for Operational Technology (OT).

Sensors on the Discovery Console for OT

The Appliance page displays a list of all Sensors and Collectors that are associated with a Discovery Console for OT.

Appliances records

The Discovery Sensor for OT is listed on the Appliances page separately from the Collector. If you select the Sensor name from the list, you can open that Sensor record. You can perform the same actions with the Sensor as you would with the Collector. However, Collectors aren't registered to the Console. For more information, see Appliances page and Edit an Appliance.

Configure the Discovery Sensor for OT

Configuring the Discovery Sensor for OT provides discovery of all assets in your OT environment. The Sensor requires a Linux operating system that is installed either as a virtual machine or on a Bare-metal computer that is x86.

Discovery Sensor for OT System requirements

System Requirements

Component	System Requirements
Discovery Sensor for OT	• 16 GB RAM • 100 GB Hard drive • 2 CPUs • 2 virtual NIC cards

Workflow

Review the steps in the Sensor installation process from the table.

Discovery Sensor for OT Installation Workflow

Task	Description
Navigate to the Download & Deploy OT Discovery page.	In the ServiceNow instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page and select Download & Deploy OT Discovery.
The **Downloads** page opens.	Download the Discovery Sensor for OT package.
EULA Agreement	Ready the EULA appears on the **Downloads** page. Accept the EULA by checking the box next to **Agree**.
ISO image	Unzip the Sensor package. The ISO image is included in the Sensor package.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Discovery Sensor for OT Installation Workflow (continued)

Create a virtual machine.	Select **Other Linux 64-bit** as the OS.
CD/DVD	Attach the Sensor ISO to the CD/DVD to boot the VM.
Run the installation.	Follow the installation steps in Install the Discovery Sensor for OT.
Register the Sensor	Register the Sensor with the DMI and Console. This confirms that the Console and Sensor can communicate with each other. For more information, see Register the Discovery Sensor for OT for more information.

Install the Discovery Sensor for OT

Download the Discovery Sensor for OT package and install the ISO image. Then install the Discovery Sensor for OT.

Before you begin

Role required: admin

About this task

You can register the Sensor after you have installed the OT Discovery Console and system. Before you can register a Sensor to the Console, you must confirm that you have completed the following.

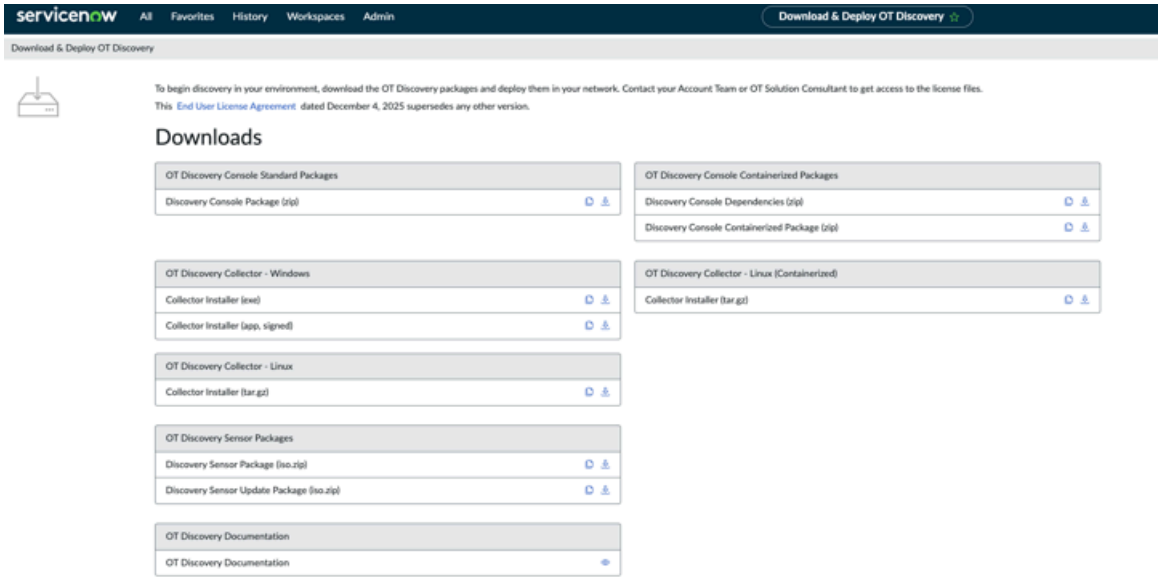
- From the Downloads page, download the Sensor package; the Sensor ISO file is in the same package.
- Install the ISO image.
- Determine if you're using the ISO as a Virtual Machine (VM) or are installing the ISO on hardware. If you're using the ISO as a VM, you can use any of the following VMs.
  - VWware
  - Hyper-V
  - Proxmox
  - Linux KVM

  If you choose to install the ISO on hardware through BareMetal, you must use a tool to create a USB ISO installer.
- You must open both the Console and the DMI interfaces to complete the Sensor registration.

Procedure

1. On your instance, navigate to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup page.
2. Select the **Get Started**.
   The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

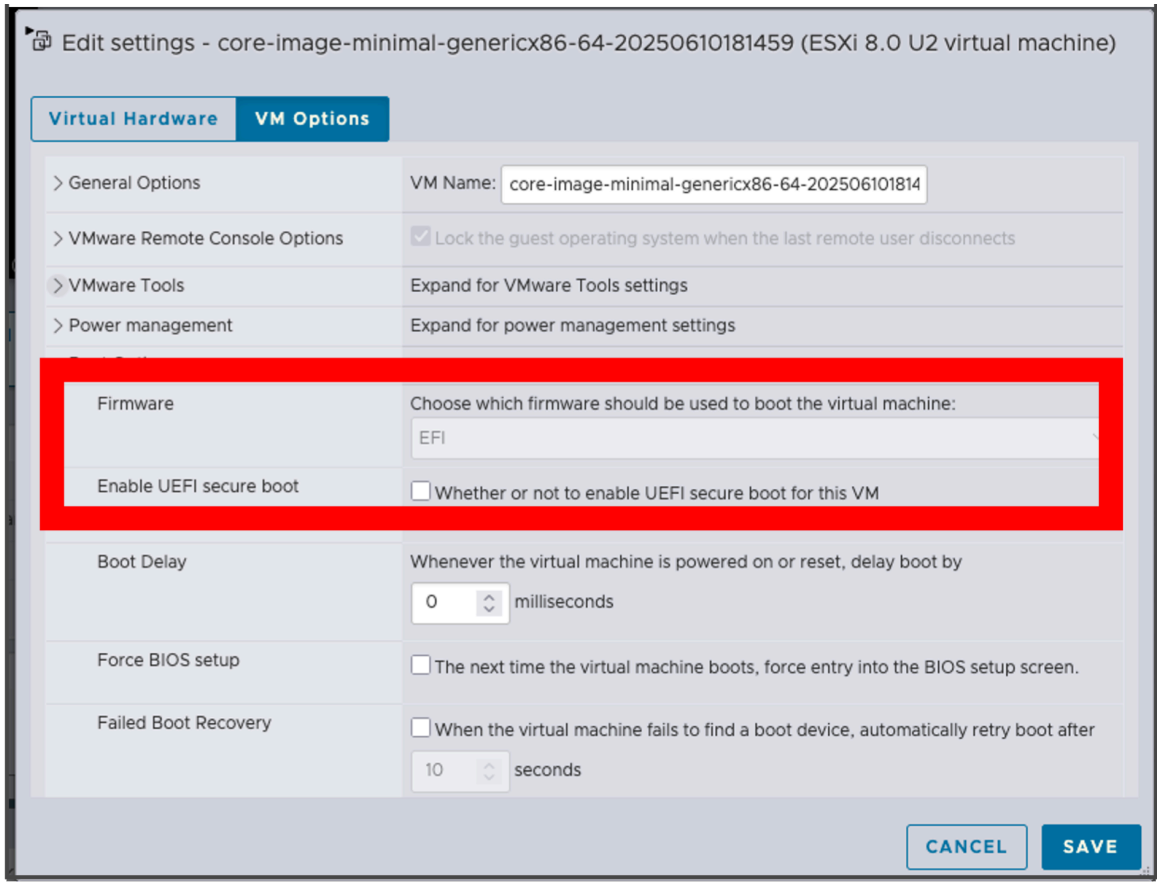


Note: Read the End User License Agreement (EULA) carefully and then check **Agree**.

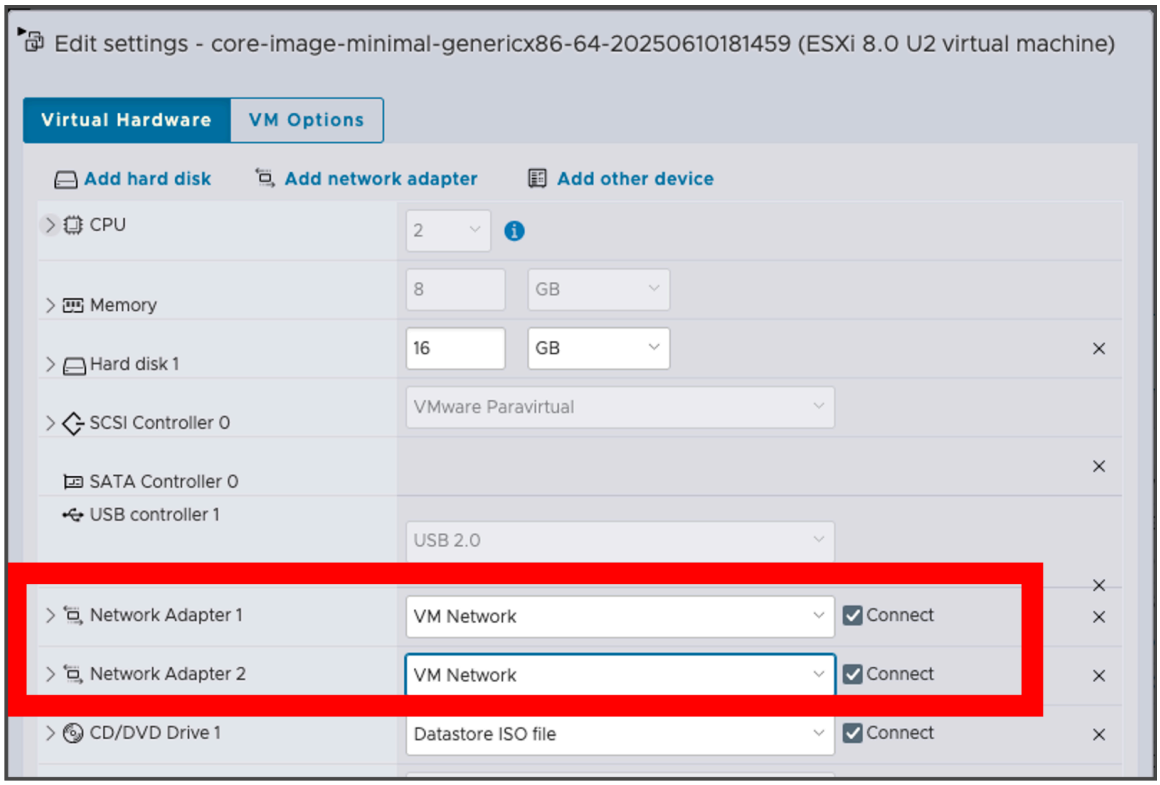
5. Download the Discovery Sensor for OT installation and deployment package.
6. Unzip the Sensor package.
   The ISO image is included in the Sensor package.
7. Create the virtual machine for the Discovery Sensor for OT.
8. Install the Discovery Sensor for OT.
9. Select the default answers for all prompts.
10. Upload the ISO image to your virtualization platform.
11. Create the hardware NICs which the VM uses to communicate with the Sensor.

Note: The following images are examples specific to an ESXi 8.0 U2 virtual machine.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



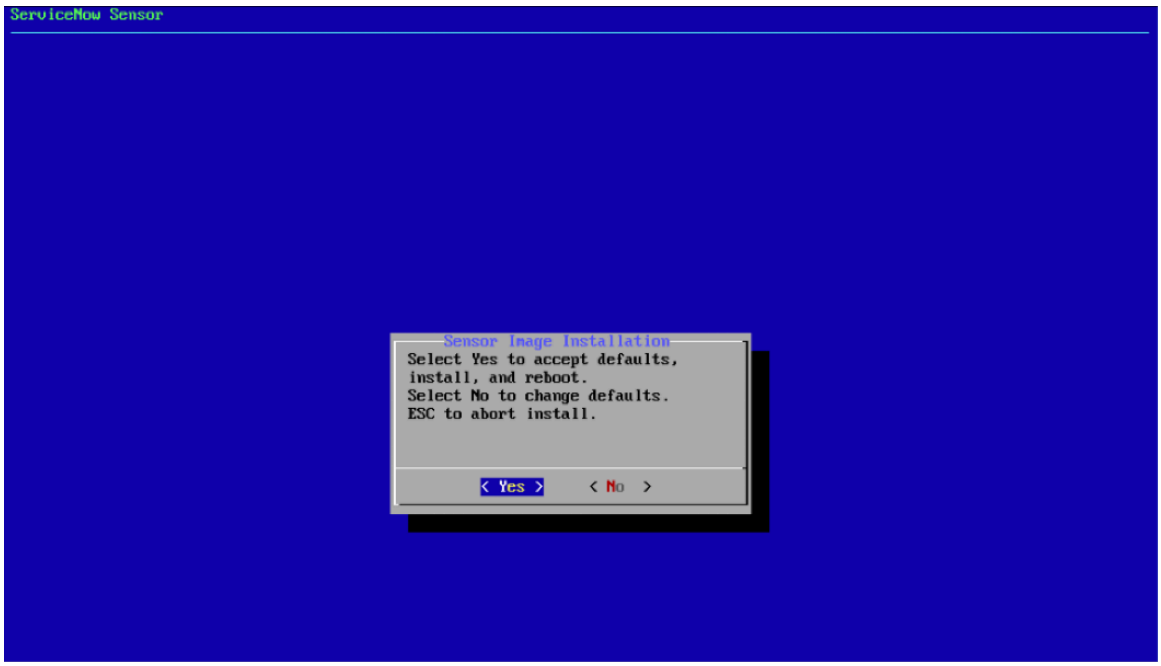
Note: For communications to work between Discovery components, two network adapters should be connected on the VM.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

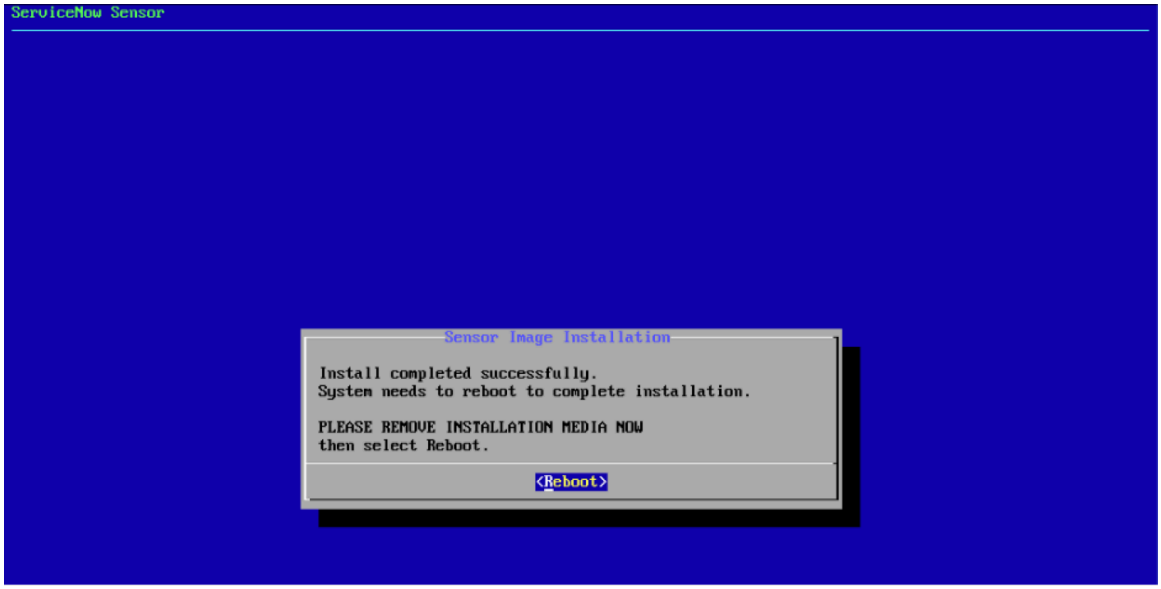
Note: For other VM options, confirm that EFI is selected (and not BIOS) as the Firmware and that the "Enable Secure Boot" flag is not selected.

12. Install the ISO image.
13. After installing, when alerted, remove any install media.
    The alert message is: "System needs to reboot to complete installation. Please remove all install media and once complete press any key to reboot."
14. Reboot the system.
15. After removing any install media, the install process starts for the Sensor.
16. Create the virtual machine for the Sensor.
17. Select the OS as **Other Linux 64-bit**.
18. Attach the Sensor ISO to the CD/DVD to boot the VM.
19. Create 2 hardware NICs specifically for the VM.
20. For other VM options, confirm that EFI is selected (and not BIOS) as the Firmware and that the "Enable Secure Boot" flag is not selected.
21. Assign a minimum of 8 GB RAM and 60 GB HDD for the installation.
22. Power on the VM and the install starts.
    You see this screen:

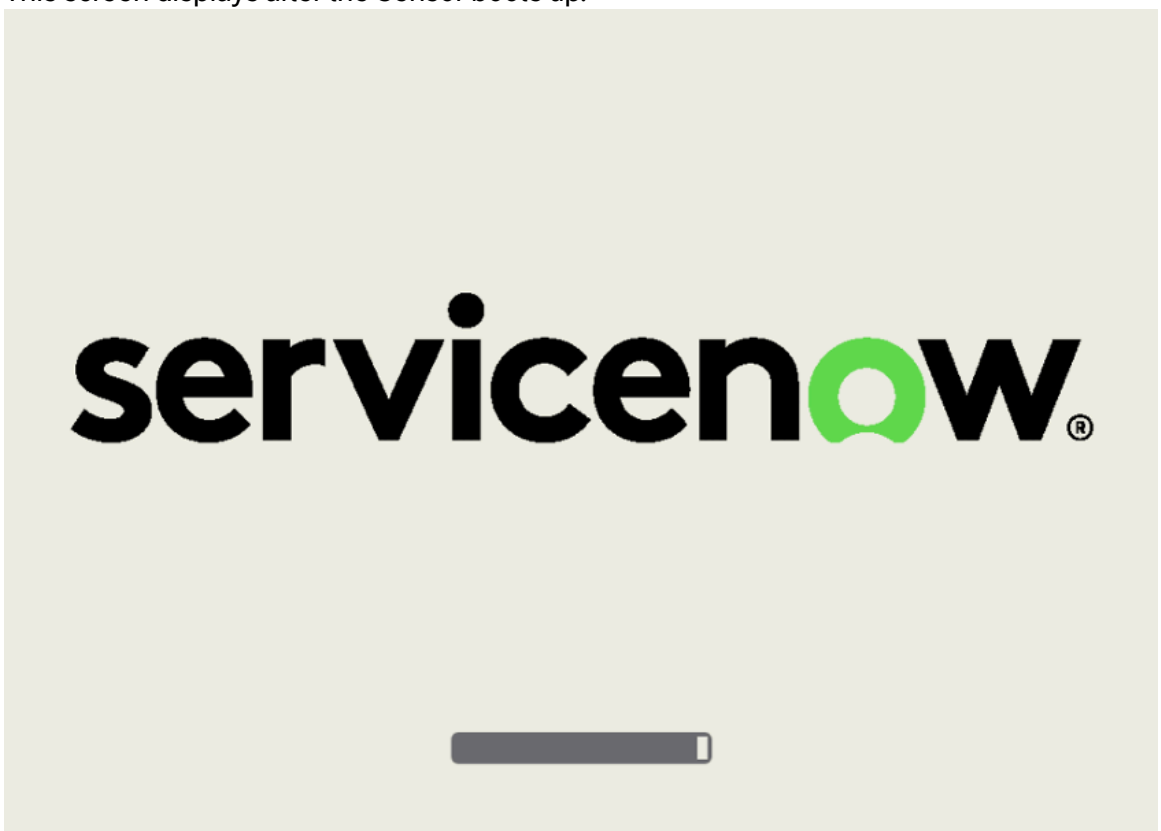


23. Select `Yes` to start the install.
24. Once the install is complete, select **Enter** to reboot the VM.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



This screen displays after the Sensor boots up.



25. On the VM page, the DMI page URL displays.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

26. Use this URL to log in to the DMI and register your Discovery Sensor for OT to the Console. For more information, see Register the Discovery Sensor for OT.

What to do next
Register the Discovery Sensor for OT

Register the Discovery Sensor for OT

When you have installed the Discovery Console for OT and the Discovery Sensor for OT, register the Sensor to the Console with the Console's Device Management Interface (DMI).

Before you begin
Role required: admin

About this task
Confirm you that you have installed the Sensor. You must register the Sensor to the Console with the DMI. The DMI is a web-based interface that lets you configure and register the Sensor with the Console. For more information on the DMI, see Device Management Interface. Registering the Sensor confirms it can communicate with the Console.

Procedure
1. Access the DMI for a Discovery Sensor for OT by opening a browser and entering the URL displayed on the screen when the Sensor is installed and boots up.

   Note: Currently, there isn't a serial number portion since there's no active hardware. These input steps are still valid. But the `[serial number]` is likely to be the Sensor name at the time of its creation. This is an example of how to find the URL for the DMI. Your IP address will be different from this example:

   ```
   https://[device type]-[serial number] with
    either .local:443 or .[domain name]:443
   ```

   Be sure to make a note of the DMI URL displayed after the Sensor is installed. You can use this URL for the DMI. This image shows the DMI URL as https://172.16.241.131:443.



2. In the DMI, log in using your credentials.
   - DMI (Web Interface):
     - Username: admin
     - Password: password
   - SSH login:
     - Username: serviceadmin
     - Password: devpassword

   Note: After the initial log in is completed, the DMI prompts you to change the password.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. In a separate tab or browser, log in to the Discovery Console for OT.
4. In the Console, navigate to **Appliances > Certificates**.
5. Under Sensor Credentials, select the **Generate Bundle**.
   In the prompt window, select **Generate Bundle** again.
6. The bundle generates and downloads to your designated download folder.
7. Switch back to the DMI.
8. In the DMI, navigate to **Console > Credentials**.
9. Select **Bundle File Input** and from this window, select the generated Sensor bundle.
10. Select **Upload Credentials Bundle** to upload the Sensor bundle to the DMI.
    After the bundle is uploaded, the **Certificate Update Logs** appears and confirms the completed process.
11. The DMI automatically extracts the certificate from the bundle and registers the Sensor.
12. From the DMI menu, select the **Network** tab.
13. Select the **Edit** button.
14. Select an IP Address or Hostname for the Console endpoint and enter a valid value.
    Enter a valid Gateway IP Address.
15. Select **Save & Deploy**.
16. Navigate back to the **Console** tab and select the **Register** button.
17. In the Console, confirm that the Sensor is online.
    The device briefly shows online and then offline. Then it shows a steady online status in the Console.

Result
The Sensor and the Console can now communicate and generate queries.

Device Management Interface

The Device Management Interface (DMI) is a web-based interface where you configure and register a Discovery Sensor for OT to the Discovery Console for OT.

DMI overview

With the DMI, registering a Sensor enables the Sensor to communicate with the Discovery Console for OT. By registering the Sensor, you're ready to start using the Console.

Note: The Console and the DMI are separate web-based interfaces that you access with an HTTPS web address. Open both interfaces when registering the Sensor. During the first log in to the DMI, the username admin and the password `devpassword` are provided.

Once the Console is deployed and you have registered the Sensor, you can create these necessary components on the Console to discover assets in your environment.

- Site
- Network Zone
- Auto Query
- Quick Scan

For more information about these Console features, see Discovery Console for Operational Technology (OT).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

DMI pages

The following sections describe the pages available on the DMI.

Device

The Device page includes a summary of the basic configuration information for the Sensor. This page includes details about the Sensor's name, type, description, serial number, firmware version, build date, model, and revision.

On the Device page, you can edit the Sensor name. If you change the name before you register the Sensor, the updated name appears in the Console. Otherwise, if you change the name after registering the Sensor, you must update the Sensor name in the Console itself.

Network

The Network page includes a diagram of the Sensor and information about its connection to the Console, management interface, and bridge or span interface. You can edit the information on this page as needed when registering the Sensor.

Console

The Console page enables you to register the Sensor with the Console. If needed, you can edit the Console endpoint and Console gateway from this page. Selecting the **Edit Settings** button redirects you to the Network page, where you can make your changes. After your register the Sensor with the Console, the Sensor appears in the Console on the Sensors page.

Location

The Location page includes the following fields that describe the location of the Sensor.

- Latitude
- Longitude
- Description of the physical location

You can add or change the location information for a Sensor by selecting the **Edit** button.

Password

ThePassword page provides the option to update the password of the DMI. You can change the password by selecting **Edit** and entering the updated password.

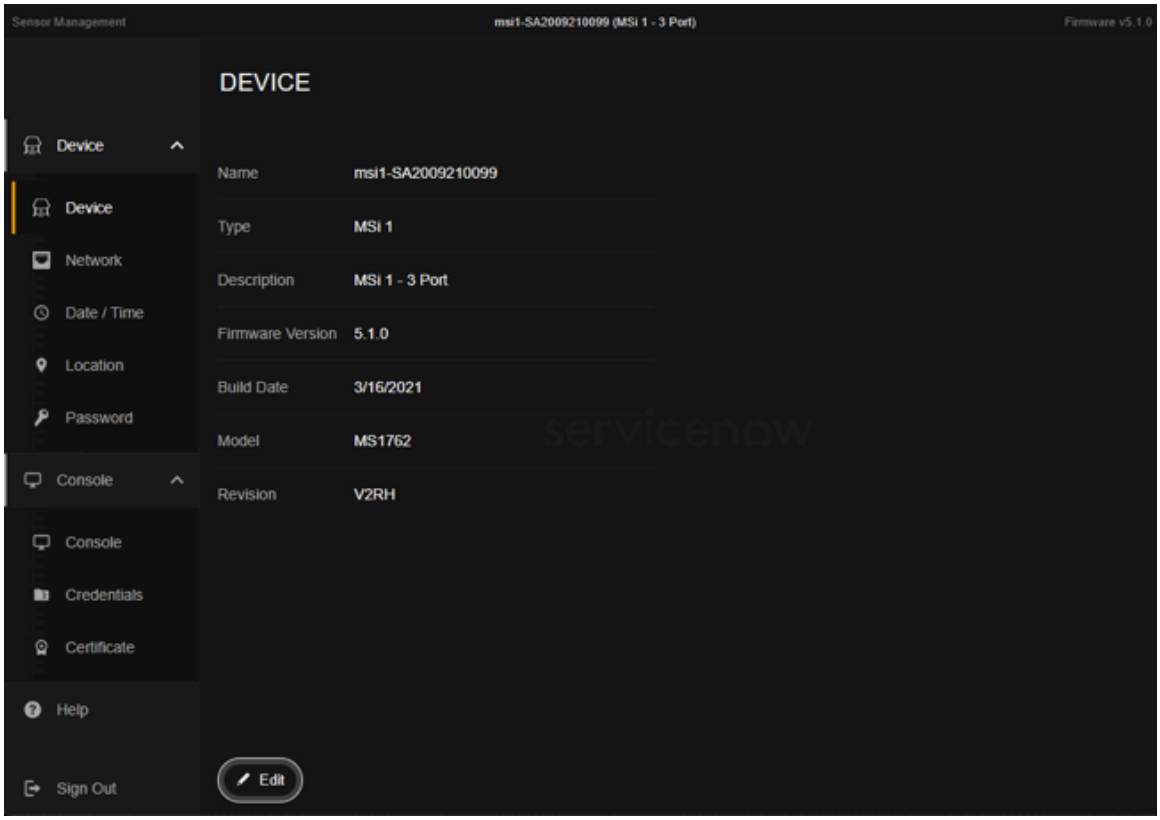
Certificate

The Certificate page enables you to upload a certificate downloaded from the Discovery Console for OT. This certificate is needed for registering the Sensor with the Discovery Console for OT.

Help

The Help page includes information about keyboard shortcuts related to the DMI.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



Deregister a Discovery Sensor for OT

Deregister a Discovery Sensor for OT from the Discovery Console for OT that is no longer available on your system.

Before you begin

Role required: admin

Procedure

1. In the Console, navigate to the Sensors page.
2. Select the Sensor that you want to deregister.
3. Select the Actions icon.
4. Select **Deregister Device**.
5. In the Deregistered Device modal window, select **Deregister**.

Result

The Sensor is deregistered, and the Sensor is reset to the default network configuration, which is the DHCP with the link-local fallback.

For removing a lost Sensor, see Remove a lost Sensor.

Remove a lost Sensor

Remove a Sensor that no longer functions or is otherwise reported as having a lost connection from the Discovery Console for OT.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

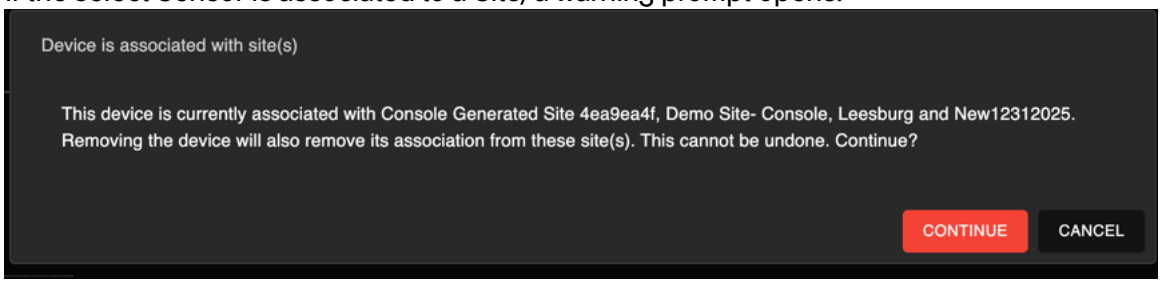
1. Navigate to the **Appliances** page.
2. From the list, under the Name column, select the Sensor that you want to remove.

> **Danger:** Removing Sensors in the OT environment may require working in environments with dangerous voltages, moving parts, and other safety hazards. Sensors should only be removed by persons with proper electrical and workplace safety training.

3. The Sensor record opens for the selected appliance.
4. In the record, select the Action button.
5. From the menu, select **Remove Device from Console**.

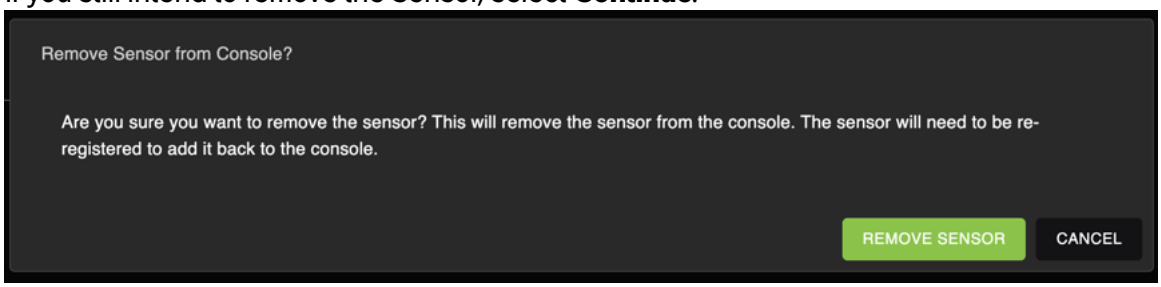
> **Note:** The **Remove Device from Console** option is only available in the drop-down if the Device Status is **Connection Lost**.

6. If the select Sensor is associated to a Site, a warning prompt opens.



Removing a Sensor that is associated to a Site can't be undone.

7. If you still intend to remove the Sensor, select **Continue**.



8. Select the **Remove Sensor** button to complete the removal.

Result

The Sensor is no longer displayed on the Discovery Sensor for OT list page. Existing network connections associated with the Sensor remain in the system for historical purposes.

> **Important:** If you remove a lost Sensor from the Console, it may still be powered on and operating at its installed location. Verify that the Sensor is properly powered down and removed from the field after removing them from the Console. If a lost Sensor is found to be operational after having been removed and must be reinstalled on the network, you must contact the Technical Support team for assistance in reconfiguring the Sensor.

Operational Technology Discovery Collector

Use the OT Discovery Collector component to discover devices the Discovery Sensor for OT can't reach in the OT environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started

Use the links in the Related Topics section to explore, configure, and use the OT Discovery Collector.

Explore the Operational Technology Discovery Collector

The OT Discovery Collector provides you with enhanced features to create an inventory of your assets in your OT environment.

OT Discovery Collector overview

The OT Discovery Collector is a lightweight software application that is used to discover devices within segments of the OT network where a Sensor can't reach. It is deployed deep within the network zones in your OT environment. The Collector delivers native protocol support without requiring any appliance, making it fast to implement and easy to scale.

Appliances records

The OT Discovery Collector is listed on the Appliances page separately from the Discovery Sensor for OT. If you select the Collector name from the list, you can open that Collector record. You can perform the same actions with the Collector as you would with the Sensor. However, you aren't required to register a Collector to the Discovery Console for OT. For more information see, Appliances page and Edit an Appliance

What to explore next

For more information about the OT Discovery Collector or to get help with the application, see:

- Configure the OT Discovery Collector
- Contact Customer Service and Support

Configure the OT Discovery Collector

The OT Discovery Collector is an application that you can install on a Windows or Linux system.

Collector Credentials

Depending on how you have deployed the Console, you may have to manually edit the hostname value in the `config.json` file to validate the Collector's credentials. If you install an offline Console or install into cloud environments, the `hostname` value may not be correct. For the OT Discovery Collector, the hostname needs to be set to the Console hosts external/network IP address. It is important to check this setting and adjust it as needed.

Note: You can now download and install Containerized Collector packages. For a Windows OS machine, be sure to select the compatible Collector OS. For more information, see Air-gapped networks and OT Discovery installation.

Collector minimum system requirements

The OT Discovery Collector can be installed and run on either a Windows OS or a Linux OS.

Component Operating System	Minimum System Requirements
Windows	The OT Discovery Collector installation is compatible with Windows 10 or Windows 11 systems.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Component Operating System	Minimum System Requirements
	The required Windows (10 or 11) environment for the OT Discovery Collector is x86_64. ARM or Apple Silicon devices aren't supported. For more information, see Install the OT Discovery Collector on a Windows system.
Linux	For more information, see Install OT Discovery Collector on a Linux system.

Install the OT Discovery Collector on a Windows system

Install the OT Discovery Collector on a Windows system. The OT Discovery Collector installation is compatible on Windows 10 or Windows 11 systems.

Before you begin

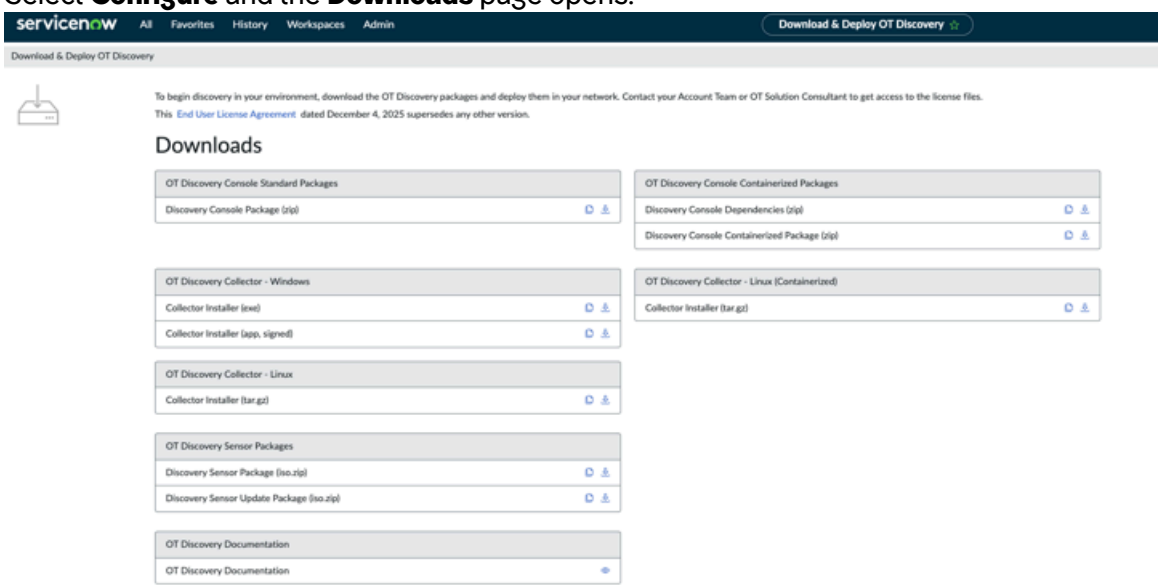
The required Windows (10 or 11) environment for the OT Discovery Collector is x86_64. No ARM/ Apple Silicon devices are supported.

Role required: admin

Note: You can now download and install Containerized Collector packages. For a Windows OS machine, be sure to select the compatible Collector OS. For more information, see Air-gapped networks and OT Discovery installation.

Procedure

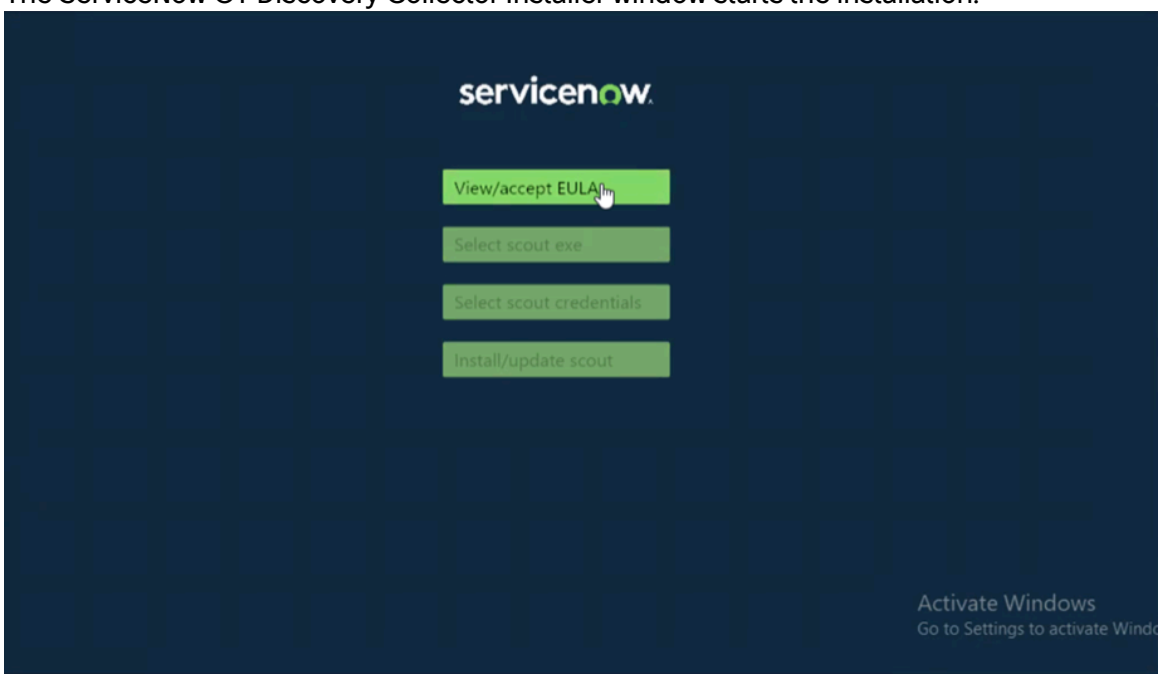
1. On your instance, navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup page.
2. Select the **Get Started**.
   The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.



Note: Read the End User License Agreement (EULA) carefully and then check **Agree**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Download the OT Discovery Collector installation and deployment package for Windows.
6. Install the Collector on the Discovery Console for OT you intend to use.
7. On the Discovery Console for OT, navigate to the **Sensors** > **Certificates** > page.
8. To generate the OT Discovery Collector credentials you need, from the list under the Bundle Password section, select the **Generate Password** button.
9. Select the radio button next to the desired **Bundle Format**.
   The recommended format is ZIP.
10. Select the **Generate Bundle** button.
    The Generate OT Discovery Collector Credential Bundle window opens.
11. Select the **Generate Bundle** button in this window.
    The `ServiceNow_OT_Discovery_Collector_Windows` bundle zip file is downloaded to your machine.
12. Extract the `ServiceNow_OT_Discovery_Collector_Windows.zip` file.
    The zip file contains a `config.json` file and a `cert` folder. The `cert` folder contains the following files:
    - `ca_root_certificate.pem`
    - `client.device.rabbit.pem`
    - `client.device.rabbit.privatekey.pem`
13. Navigate to the `ServiceNow_OT_Discovery_Collector_Windows_Installer_[datestamp]` folder.
14. In this folder, select and hold the right key on the `ServiceNow_OT_Discovery_Collector_Windows_Installer` file and select **Run as Administrator**.
15. When prompted, select **Yes** to enable this app to change to your computer.
    The ServiceNow OT Discovery Collector Installer window starts the installation.

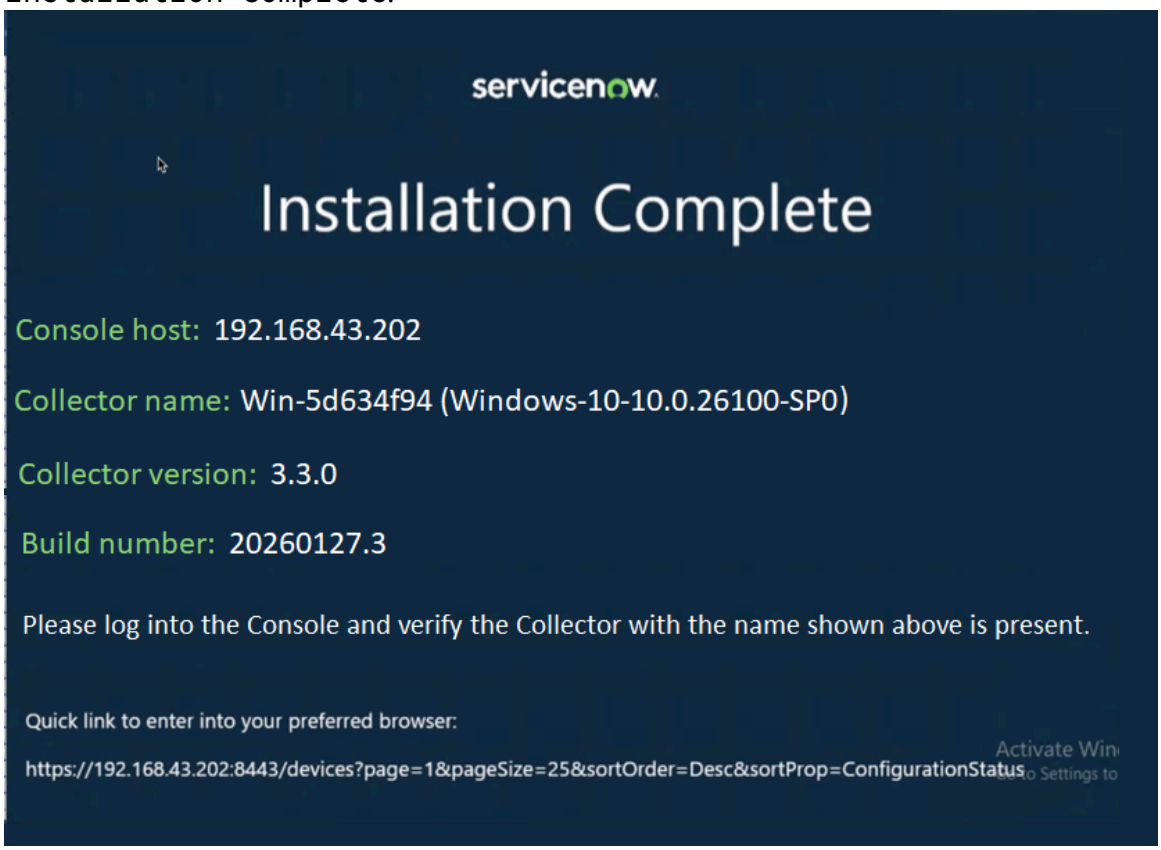


16. Select the **View/accept EULA** button to accept the End User License Agreement (EULA).
    Read the EULA carefully. If you don't agree to the EULA, or skip this step, the installation is canceled.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you accept the EULA, a dialog window pops up.

17. In the dialog window, select the `SNDiscoveryCollector_install_windows` file and select **OK**.
18. Select the **Select** *`OT Discovery Collector`* **Credentials** button.
    After you select this button, a dialog window opens.
19. In the window, select the `collectorBundle` file and select **OK**.
20. Select the **Install/Update Collector** button on the installation screen.
    When complete, the ServiceNow OT Discovery Collector Installer window displays `Installation Complete`.



21. Navigate to your local disk program files folder, so that you can see the `SNDiscoveryCollector` folder is present.
22. **Optional:** Navigate back to the Download & Deploy OT Discovery page and select **Mark as complete**.

Result

In the Discovery Console for OT window, the OT Discovery Collector appears on the Discovery Sensor for OT screen.

The OT Discovery Collector is installed on your Discovery Console.

What to do next

To update the OT Discovery Collector version, do the following steps.

1. Re-run the installer.
2. Select the latest version of the OT Discovery Collector.
3. Use the same credentials again.
4. Select the **Install/Update** *`OT Discovery Collector`* button.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The updated version is installed.

Install OT Discovery Collector on a Linux system

Install the OT Discovery Collector on a Linux system.

Before you begin

- SCP the `linuxCollectorinstaller_[version number]_[build number].tar.gz` over to the Linux system.

  Note: An example of the file name format is `linuxCollectorinstaller_3.3.1_20250917.1.tar.gz`.

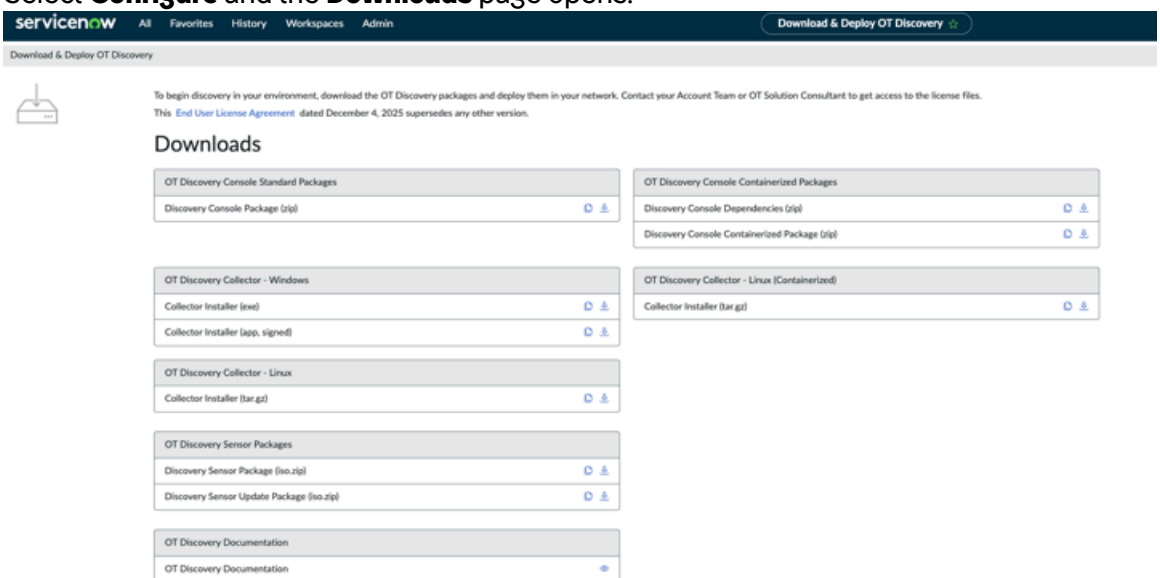
- SCP the `CollectorBundle` file you generated and downloaded from the Discovery Console to the Linux system.
- To go into OT Discovery Collector Linux host, use `ssh`.
- Use `su` or `sudo -s` to switch to the root user.

Role required: admin

Note: You can now download and install Containerized Collector packages. For a Windows OS machine, be sure to select the compatible Collector OS. For more information, see Air-gapped networks and OT Discovery installation.

Procedure

1. On your instance, navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup page.
2. Select the **Get Started**.
   The **Download & Deploy OT Discovery** page opens.
3. In the first section of the setup, select **Download & Deploy OT Discovery**.
4. Select **Configure** and the **Downloads** page opens.



Note: Read the End User License Agreement (EULA) carefully and then check **Agree**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Download the OT Discovery Collector installation and deployment package for Linux.
6. Install the Collector on the Discovery Console for OT you intend to use.
7. On a RHEL-based distribution, install tar.

```
sudo dnf install -y tar
```

8. On all Linux distributions, run the following command:

```
tar -xvf linuxCollectorinstaller_[version number]_[build
 number].tar.gz
```

9. Copy the `CollectorBundle` file into the `CollectorInstaller` directory.

```
chmod +x Collector-init.sh

./Collector-init.sh
```

10. When the script starts, the system locates the pdf version of the EULA.

    When prompted to accept the EULA, enter `Y` for yes.

11. After the script completes successfully, the OT Discovery Collector can be seen in the console.

    To check the service status, run this command: `systemctl status SNDiscoveryCollector`. If you would like to view the journal output for the service to troubleshoot issues, as the root user you can run `journalctl -f -a -u SNDiscoveryCollector`.

Result
After the script completes successfully, the OT Discovery Collector can now be seen in the console.

To check the service status, run this command:

```
systemctl status SNDiscoveryCollector
```

.

If you would like to view the journal output for the service (usually as a troubleshooting measure), as the root user you can run:

```
journalctl -f -a -u SNDiscoveryCollector
```

.

Use the OT Discovery Collector

When your OT Discovery Collector stops or loses power use the next task specific to your OS to restart it.

Helpful Tasks

Use the links in the Related Topics section to do the tasks needed when your OT Discovery Collector stops or loses power.

- Restart OT Discovery Collector on a Windows system
- Restart OT Discovery Collector on a Linux system

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Restart OT Discovery Collector on a Windows system

Perform manual restart of the OT Discovery Collector when its configuration file has been refreshed, or if it is unstable. You can perform manual restart only on Collectors installed in a Windows environment and for Linux-based agents that use `systemd`.

Before you begin
Role required: admin

Procedure

1. On a windows system, navigate to the host where the OT Discovery Collector is running.
2. Open the Services dialog in Windows.
3. Select SNDiscoveryCollectors.
4. Select **Restart the service**.

Result
The OT Discovery Collector restarts in the Windows environment.

Restart OT Discovery Collector on a Linux system

Perform manual restart of OT Discovery Collector when its configuration file has been refreshed, or if the OT Discovery Collector is unstable. You can perform manual restart only on the Collector installed in a Windows environment and for Linux-based agents that use `systemd`.

Before you begin
Role required: admin

Procedure

1. Use SSH to access the Linux host.
2. Use `sudo` or `su` to run the following command with root permissions.

```
systemctl restart SNDiscoveryCollectors
```

Result
The OT Discovery Collector restarts in the Linux environment.

Service Graph Connector for ServiceNow Operational Technology (OT) Discovery

The Service Graph Connector for ServiceNow Operational Technology (OT) Discovery (SGC) imports data from a connected Operational Technology Discovery OT Discovery environment and leverages the Integration Hub ETL framework.

Use the links in the Related Topics section, to explore and configure the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery.

Troubleshooting

If you have any errors or difficulties while using the Service Graph Connector, Contact Customer Service and Support.

Explore the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery

The Service Graph Connector for ServiceNow Operational Technology (OT) Discovery imports data from a connected Operational Technology (OT) Discovery environment and leverages the Integration Hub ETL framework.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

Go through each step to install and setup the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery (SGC).

Service Graph Connector for ServiceNow Operational Technology (OT) Discovery prerequisites and settings

During set up of the Discovery Console for OT, review and confirm you have the following settings.

Dependencies and requirements

Confirm you have these settings and then follow the Discovery Console for OT Guided Setup.

Dependencies and requirements:

- The Industrial Core plugin.
- The ISA Equipment Model store app with a minimum version of 1.0.11.
- The ITOM Discovery License plugin (com.snc.itom.discovery.license). You must activate this plugin.
- ITOM Licensing plugin (com.snc.itom.license). For more information, see Request Discovery.
- The Datastream Action plugin (com.glide.hub.action_type.datastream), which is automatically installed.

Install the Service Graph Connector for ServiceNow OT Discovery Service Graph Connector for ServiceNow

Install the Service Graph Connector for ServiceNow OT Discovery from the ServiceNow Store.

Before you begin

Role required: admin

Procedure

1. In the ServiceNow Store, select **Get** on the Service Graph Connector for ServiceNow OT Discovery store page to entitle the integration to one or more ServiceNow instances.
2. Once entitled, log in to your instance.
3. Navigate to **System Applications** > **All Available Applications** > **All**.
4. Locate the Service Graph Connector for ServiceNow OT Discovery and select **Install**.

Result

The Service Graph Connector for ServiceNow OT Discovery application is installed on your system.

What to do next

Navigate to the Service Graph Connector for ServiceNow OT Discovery Guided Setup. This guides you through all the mandatory and optional steps to setting up the Service Graph Connector.

Service Graph Connector for ServiceNow OT Discovery Guided Setup

Use the Guided Setup for the Service Graph Connector for ServiceNow OT Discovery to lead you through the installation, connection, configuration, and integration steps for the OT Discovery environment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

Review the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery prerequisites and settings section before beginning.

Role required: admin

Procedure

1. From your ServiceNow instance, navigate the **All** menu.
2. Enter `Service Graph Connector` into the filter and scroll down the menu to find ServiceNow OT Discovery.
3. Select **Setup**.
4. The Service Graph Connector for ServiceNow OT Discovery Guided Setup page opens.
5. On the Guided Setup page, select **Get started**.
   This opens the page with each task for downloading the OT devices and steps to configure connections, integrations, and imports for the Service Graph Connector.
6. In the first section, select **Download & Deploy OT Discovery**.
   This opens the **Download & Deploy OT Discovery** page.
7. Select **Configure**.
8. Read the EULA and then download the packages for the Console, Sensor, and Collector.
9. Choose the OT Discovery Collector OS package that matches your machine's OS.

   Note: If you have a closed network, download the Sensor package and the containerized versions of the Console and Collector packages. When ready, in stall the Console first, install the Sensor after that and, finally, install the Collector. For more information, see Air-gapped networks and OT Discovery installation.

10. Return to the previous page and select **Mark as complete**.
11. Go back to the Service Graph Connector Guided Setup page.
12. The next section is **Configure table permissions**.

    Note: Setting the table permissions allows you to have multiple connections across multiple consoles. This depends on your deployment choice of the Discovery Console for OT.

    a. In the Configure table permissions section, select **Scheduled data import**.
    This opens the Configure table permissions page.

    b. Next to the **Scheduled data import** task, select **Configure**.

    c. The Scheduled data import table opens.

    d. In the table, select the **Application Access** tab.

    e. Confirm that the Can Read, Can Create, and Can Update options are checked.

    f. Select **Update**.

    g. Return to the Configure table permissions page and select **Mark as complete** next to the **Scheduled data import** task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

h. Select **Configure** next to the **Data source** task.

i. The Data source table displays.

j. Select the **Application Access** tab.

k. Confirm that Can Read, Can Create, and Can Update options are checked.

l. Select **Update** or **Save**,

m. Return to the Configure table permissions page and select **Mark as complete** next to the **Data source** task.

n. Return to the Guided Setup page.

Note: These settings give you flexibility in how you setup your system. The Service Graph Connector for ServiceNow OT Discovery supports multiple-connections to multiple consoles. This depends on the deployment choice made for the Consoles. These settings give you the ability to create multiple data source objects, console objects, and multiple schedules from which to pull data.

What to do next

The next step in the Guided Setup is Configure the OT Discovery connections & credentials.

Configure the OT Discovery connections & credentials

Configure the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery authentication credentials and configuration used to connect to the ServiceNow OT Discovery devices.

Before you begin

Role required: admin

Note: It's recommended that you switch to the application scope toService Graph Connector for ServiceNow Operational Technology (OT) Discovery.

Procedure

1. Confirm that the application scope is set to the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery by using the application picker.
2. Under **Configure the connection** section only configuring the MID Server is optional.

   Note: The MID Server is required when the console can't be reached from the internet. If the console is reachable to the ServiceNow instance then MID Server is not needed.

3. Download and install the MID Server on the host machine, test the connection, and then validate the MID Server.
   Configure the MID Server using the MID Server Guided Setup.

   The MID Server access is a secure proxy between the ServiceNow Instance and the Console, allowing ServiceNow to schedule jobs and make REST calls into the environment to pull various pieces of information such as Assets, installed software, and so on. Without the MID Server, ServiceNow can't initiate direct communication if the Discovery Console is not reachable from the ServiceNow Instance

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

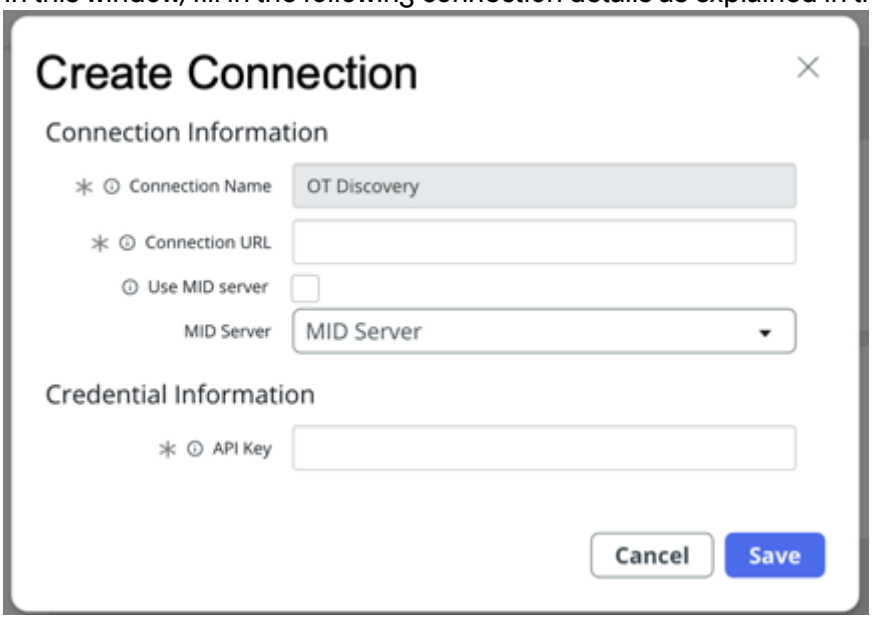
4. Use the MID Server certificate check policies link to review the policies.

   Note: Enable/Disable the required security policies for the MID Server based on the network configuration.

5. Next to the **Configure the OT Discovery Connection & Credentials** task, select **Configure**.

   Note: Depending on your ServiceNow version, you're directed to Workflow Studio or the Workflow Studio Connections list. The Outbound connections are listed in alphabetical order.

6. Navigate to or search for the OT Discovery Connections record.
7. You can view and edit connections by selecting **View Details**.
   OT Discovery is the default connection.
8. On the OT Discovery connection page, select **Configure**.
   The **Create Connection** window opens. To create a connection, select **Add Connection**.
9. In this window, fill in the following connection details as explained in the following table.



Connection details

Field	Description
Connection Name	Enter a unique name for the connection. The default connection has the name as OT Discovery and is read-only. For additional connections, enter a unique name for each. This field is mandatory.
Connection URL	Navigate to the Console and copy its URL and paste it into the Connection URL field. For example: https://OTDiscoveryConsole.net:8443/ This field is mandatory.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Use MID Server	Optionally, check this box to use a MID Server for the connection.
MID Server	Optionally, select a MID Server for the connection.
API Key	To get the API Key: **a.** Go to your Console and navigate to the **Settings** page. **b.** Open the **API** tab and select the Add  icon. **c.** In the **Generate API Token** window, select the expiration length you want and select **Generate Token**. **d.** The generated token is listed in the Active token list. **e.** Select the Copy icon to copy the token. **f.** Paste the token key into the **API Key** field. **g.** Select **Save**. This field is mandatory.

10. Navigate back to the **Configure the connection** page and select **Mark as complete**.

What to do next
The next step is to Generate imports and validate the connections.

Generate imports and validate the connections

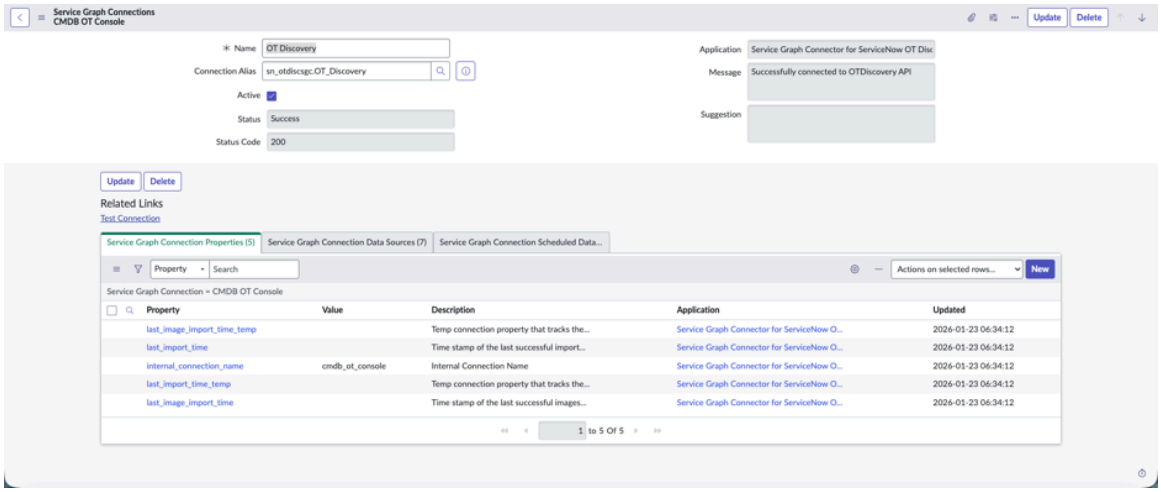
For each ServiceNow OT Discovery connection, configure the **name** and **run** as user for each import job. Each connection will generate a new **Scheduled Import Set** and **Data Source**.

Before you begin
Role required: admin

Procedure

1. Next to the **Generate imports** task, select **Configure**.
   The Generate imports for the OT Discovery Connection page opens.
2. In the **Run As User** field, select System administrator.
   This is the role within the platform who will run the schedules.
3. Select **Generate**.
   Because the Table permissions were set to Can Read, Can Create, and Can Update, this starts creating scheduled jobs in the background.
4. When finished, the banner at the top of the page states "Successfully generated import objects for connection OT Discovery."
5. Return to the Guided Setup and select **Mark as complete** next to the Generate imports task.
6. For the **Validate the connection** section, select **Configure**.
7. On the next page, check the box next to OT Discovery.
8. Under the header, **Related Links**, select **Test Connection**
9. Testing the connection takes a few moments and once completed, the page refreshes to show the test results.
   The connection is successful if the Status Code is 200. If there's an Error Code and Error Message, the connection failed and further troubleshooting is required.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



10. Select the OT Discovery link.
    This opens the Service Graph Connector OT Discovery view.
11. The table lists the connection properties, the data sources that were generated and the 7 import schedules that were created.
12. This task tests:
    - Is the Service Graph Connector able to reach the Instance.
    - If so, is there a valid license on the Console.

    If the connection was successful, but the Console license has expired, you may see a message in the Suggestion field asking you to reach out to your account representative.
13. Return to the Validate the connection section and select **Mark as complete**.
14. Return to the Guided Setup page.

Review and configure integration settings

To make the Service Graph Connector for ServiceNow OT Discovery simple to use, set options that let you modify the integration behavior to meet your business needs.

Before you begin

Be sure to complete all previous configurations for the Service Graph Connector for ServiceNow OT Discovery before beginning the following tasks.

Role required: admin

About this task

Configure the ServiceNow OT Discovery Classification Settings which define how ServiceNow OT Discovery categories are mapped to target CMDB classes. Configure additional settings based on Classification such as the CI naming strategy and if you permit OS classification. Default recommended classification settings are provided by the application which you can then configure for your needs.

Procedure

1. Select **Configure classification settings**.
   a. Next to the Configure classification settings task, select **Configure**.
   b. Review the default OT Discovery Classification Settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The OT Discovery Classification Settings define how OT Discovery categories are mapped to the target ServiceNow Instance CMDB classes. It also defines how they are configured to additional settings based on classification, such as the configuration item (CI) naming strategy and whether to permit OS classification. The default recommended classification settings are provided by the application, which you can then configure for your needs.

c. All the devices that are imported follow a default naming strategy.

d. You have the flexibility at a class level to change the name.

e. You can map the Target CMDG Class name to an OT Device type and can change the mapping settings.

f. If any changes are needed, open the OT Discovery Classification Setting record and update the entries in the following fields.

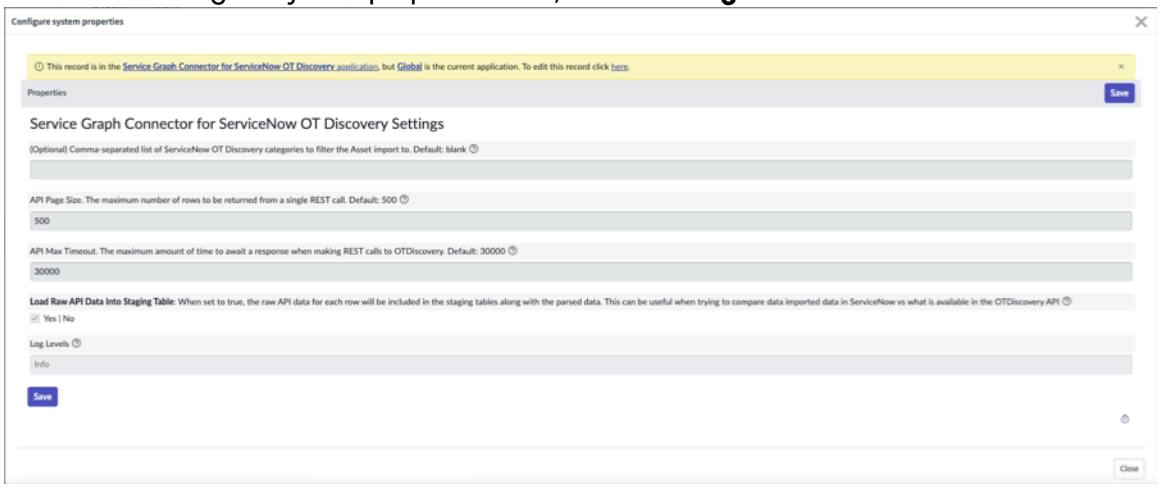
OT Discovery Classification Setting fields

Field	Description
Active	If checked, the Classification Setting is used when classifying the devices. If unchecked, the Classification Setting is ignored.
Source Class	The class name of the source asset.
Network type	Defines whether this classification setting is for OT or IT devices only. Leave empty to include both types. If OT devices with a specific category must be classified into a separate class from IT devices, there are two definitions for the OT Discovery Category. One definition has the Network type set to **OT** with the classification for the OT devices. The other definition is set to **IT** for classifying the IT devices.
Target CMDB class	The CMDB class to target when importing the OT Discovery device.
OT device type	For OT devices, you can select the OT device type to apply the device type to the imported OT Discovery asset in the CMDB, if applicable.

2. **Optional:** Next, **Configure system properties**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Next to the Configure system properties task, select **Configure**.



b. The Configure System properties window opens.

c. Review the System properties and adjust as needed for your instance configuration.

System properties

System property	Description
(Optional) Comma-separated list of OT Discovery categories to filter the Asset imports.	Filters the Asset import to only import assets of particular categories. For example, if you wanted to only import ICS Host and PLC category devices from the Discovery Console for OT, you could set this to `PLC,IcsHost`. Default: empty **Note:** These are categories defined on the Console side.
API Page Size	Maximum number of rows to be returned from a single REST call. (Optional) Default: 500
API Max Timeout	Maximum amount of time to wait for a response when making REST calls to OT Discovery. Default: 30000
Load Raw API Data into Staging Table	When set to true, the raw API data for each row is included in the staging tables along with the parsed data. This is useful when trying to compare data imported data into ServiceNow vs. what is available in the OT Discovery API.
Log Levels	Logging level verbosity to use for the application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System property	Description
	(Optional) Default: Info

d. Select **Save** and close the window.

e. Return to the Configure system properties task and select **Mark as complete**.

f. Return to the Guided Setup page.

What to do next

The next setup step is toSet up scheduled import jobs.

Set up scheduled import jobs

Configure the scheduled import jobs.

Before you begin

Role required: admin

Procedure

1. In the Setup scheduled import jobs section select **Import sites**.
   a. Next to the Import sites task, select **Configure**.
   b. Select the Site Scheduled Data Import Job.
   c. To manually execute the job, select **Execute Now**.
   d. Return to the Guided Setup and select **Mark as complete** next to the Import sites task.
   e. Next, in the Configure site mappings task, select **Configure**.
   f. Review the list of imported sites.
   g. Select the first site and in the form, fill in the following fields.
      - All field titles with * (asterick) next to them are mandatory and should be filled in.
      - Populate the **Site type** field. This field is mandatory. The value can be either OT or IT. If you select OT, all the hardware records imported later will also have OT device (cmdb_ot_entity) records related to them automatically. For any site with a Site type between IT and OT, set the **Site type** to **OT**.
      - Set the ISA assignment site. All the data in the site will import to the ISA assignment site you choose.
      - If applicable, populate the **Location** and **Company** fields.
      - Check the Active box.
      - Fill in the **Assigned Meta Data** section. Whatever you assign as Meta Data is copied onto all imported devices.

        Note: Any value populated will be cascaded down to all CIs this Site is related to when the asset data is imported into the CMDB.

   h. Select **Update**.
   i. Return to the Guided Setup and select **Mark as complete**.
2. Do the **Configure scheduled jobs** task next.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

By default, the ServiceNow OT Discovery scheduled jobs created during installation are inactive. All other jobs are configured to run after their parent job, the Site Scheduled Data Import Job. The only exception is the Asset Image import jobs, which run independently.

a. Next to the Configure scheduled job task, select **Configure**.

b. In the Scheduled Jobs list, open a site record.

c. To activate the scheduled job, select the check box next to the **Active** field.

d. In the **Run** and **Time** fields, select how often and when you want the job to run.

For example, daily at midnight.

e. Select **Update**.

f. Repeat these steps for each site in the Scheduled Jobs list.

g. When you finish the sites, select the asset record from the Scheduled Jobs list.

h. To activate the scheduled job, select the check box next to the **Active** field.

Note: You don't have to set the **Run** field for the asset record since the asset scheduled job automatically runs after the site scheduled job runs.

The following schedules jobs are available to import data:

- **Asset import**: This imports the OT Devices discovered into CMDB.
- **Network Zone import**: This imports the list of Managed Networks defined within the Site to support the deployment of OT Discovery.
- **Sensor import**: This imports list of all the Sensors used for OT Discovery deployment into the NIDS table.
- **Connection import**: This imports the list of communications between the devices.
- **Asset Images**: This imports the list of screenshots captured during the discovery process in the cmn_media table.

i. Return to the Guided Setup and select **Mark as complete** next to the Configure scheduled job task.

3. Review imported data.

a. Wait until the scheduled jobs are complete on their schedule or open the scheduled job and select **Execute Now** to execute it on demand.

b. Once the jobs are complete, select **Configure** next to the Review imported data task.

c. Review the imported CMDB data.

d. Return to the Guided Setup and select **Mark as complete** next to the Review imported data task.

Result

You have completed the Service Graph Connector for ServiceNow OT Discovery Guided Setup. Review the Use advanced configurations section.

Use advanced configurations

Use the advanced configuration for the Service Graph Connector for ServiceNow OT Discovery to set up an asset extension points, a class calculator extension points, and a configuration item (CI) naming strategy extension points.

Before you begin

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

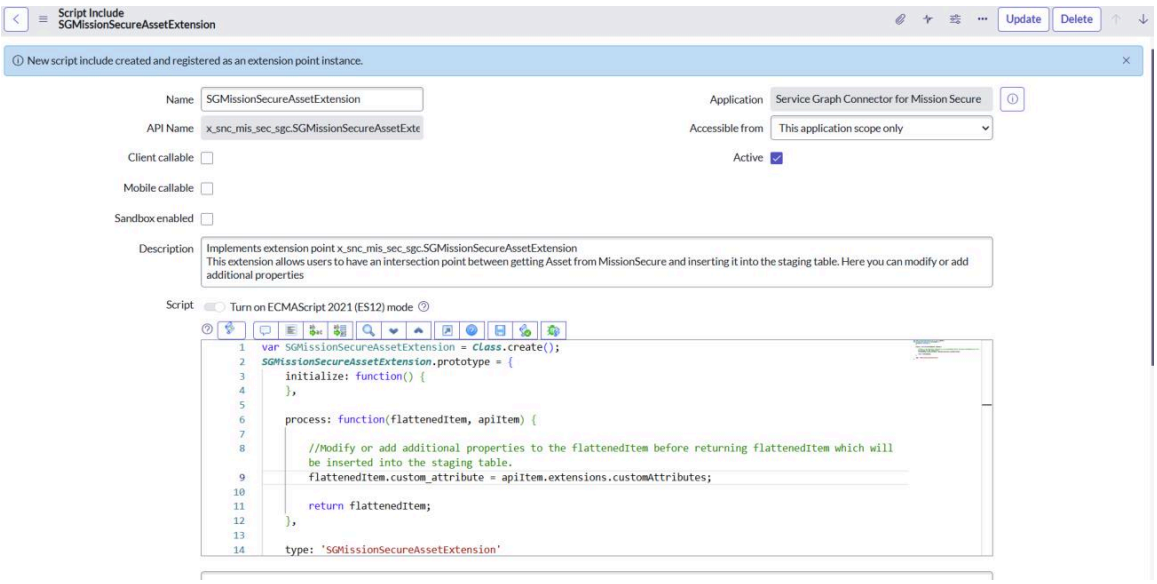
1. **Optional:** Set up an asset extension point.
   Before being transformed by the Robust Transformer (RTE) and the Integration Hub ETL, the assets from the OT Discovery API are flattened into a standard format. If you want to include additional custom attributes into the flattened asset, you can choose to use the Asset Extension Point script. Once the extension point is implemented, you can transform and map the additional custom attributes using the Integration Hub ETL.

   a. Navigate to **All** > **Service Graph Connectors** > *OT Discovery* > **Extension Points**

   b. Select the **x_snc_mis_sec_sgc.SGMissionSecureAssetExtension** record.

   c. In the Related Links section, select **Create implementation**

   d. In the script, update the process function to include the desired additional attributes using JavaScript.
   The following image is an example of a `custom_attribute` being added to the flattened asset.



   e. Once the script is complete, validate the data by running a test load of the Data Source.

   f. After you run the test load, navigate to **All** > **System Import Sets** > **SG-*OT Discovery*** > **Asset**.

   g. Validate that the Data column contains the `custom_attribute` that you added in step 1d. If the custom attribute doesn't appear, compare the `api_data` to the data to correct the issue with your code.

   h. Navigate to **Configuration** > **IntegrationHub ETL**.

   i. Under CMDB Application SG-OT Discovery, select the **SG-*OT Discovery* Asset** record.

   j. Under **1. Specify Basic Details**, select **Import Source Data and Provide Basic Details**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

k. Confirm that Integration Hub ETL is using a sample import with the **custom_attribute** from the previous step or scroll down and use the **Auto-pull a new import set** option.

l. Select **Save** and **Mark as Complete** to retrieve the import set.

> **Note:** You may see error messages when navigating back to the ETL Transform Map Assistant. You can ignore these messages.

m. Use **Preview and Prepare Data** and select **CMDB Classes to Map Source Data** to transform and map the custom_attribute as desired.

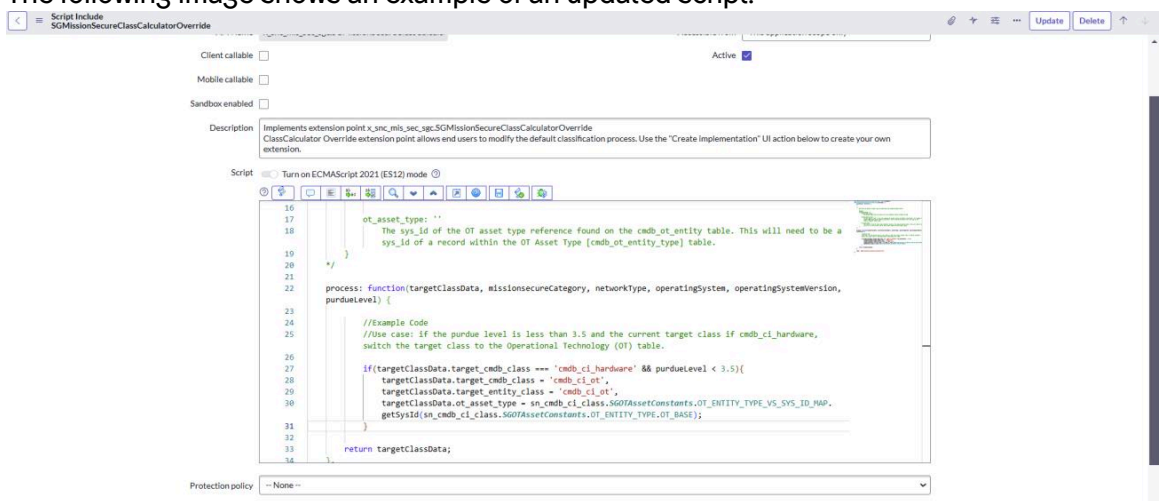
2. **Optional:** Set up a class calculator extension point.
During transformation, classification of assets from the OT Discovery API is calculated based on the OT Discovery category and, optionally, the Network type of the Site (OT orIT) using the OT Discovery Classification Settings. An extension point is provided for additional advanced configuration which overrides the classification setting.

a. Navigate to **All** > **Service Graph Connectors** > **OT Discovery** > **Extension Points**.

b. Select the **x_snc_mis_sec_sgc. SGMissionSecureClassCalculatorOverride** record.

c. In the Related Links section, select **Create implementation**.

d. In the script, update the process function as desired.
The following image shows an example of an updated script.



3. **Optional:** Set up a configuration item (CI) Naming Strategy extension point.
The Service Graph Connector for OT Discovery comes with **JustNameFallbackIPAddressAndNetworkZone**, which is a default CI Naming Strategy. If you want to name the CIs differently, you can configure additional CI Naming Strategies using the extension point.

a. Navigate to **All** > **Service Graph Connectors** > **OT Discovery** > **Extension Points**

b. Select the **x_snc_mis_sec_sgc. SGMissionSecureCINameCalculation** record.

c. In the Related Links section, select **Create implementation**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. In the script include, update the following fields.
   - Update the **Name** field to an appropriate name for the CI Naming Strategy.

     You must start the name with **SGOTDiscoveryCINameCalculation** and add the rest of the name using camel-casing with no spaces or special characters. For example, `SGOTDiscoveryCINameCalculationAppendMAC`.
   - In the **Script** field, update the `calculateCIName` function as needed.

e. Navigate to **Service Graph Connectors** > **OT Discovery** > **Classification Settings**.

f. Select the record that uses the new naming strategy.

g. Change the **CI naming strategy** field to the new CI Naming Strategy.

h. Repeat needed steps for any additional classification settings that should use your CI Naming Strategy.

Review additional Service Graph Connector for ServiceNow Operational Technology (OT) Discovery records

After completing the Service Graph Connector for ServiceNow Operational Technology (OT) Discovery Guided Setup, review the unknown devices and log records.

Before you begin
Role required: admin

About this task
These are optional tasks.

Procedure
1. On your dashboard, navigate to **All > Service Graph Connector > ServiceNow OT Discovery**.
2. In the ServiceNow OT Discovery menu, you can review extended information about and settings for the Service Graph Connector for ServiceNow OT Discovery.
3. Scroll the topics under **ServiceNow OT Discovery** until you find **All Unknown OT Devices Missing Model & Manufacturer**.
   This is a list of all the OT devices that were imported without a model number or name of their manufacturer.
4. Scroll the topics under **ServiceNow OT Discovery** until you find **All Unknown OT Devices Missing Model**.
   This is a list of all the OT devices that were imported without a model number.
5. In the menu, scroll down to **App Logs**.
   The App Log lists logs for all the OT Discovery applications within the Service Graph Connector scope. The columns are the creation date, the level, the log message, the App Scope, and the Source Script.
6. Now scroll to the **Last Imported Logs** entry in the menu.
   The table lists a creation date, what the level of the message is, whether information or warning, and the source of the entry.
7. Use the items in the menu to review information from the Service Graph Connector for ServiceNow OT Discovery Guided Setup settings.

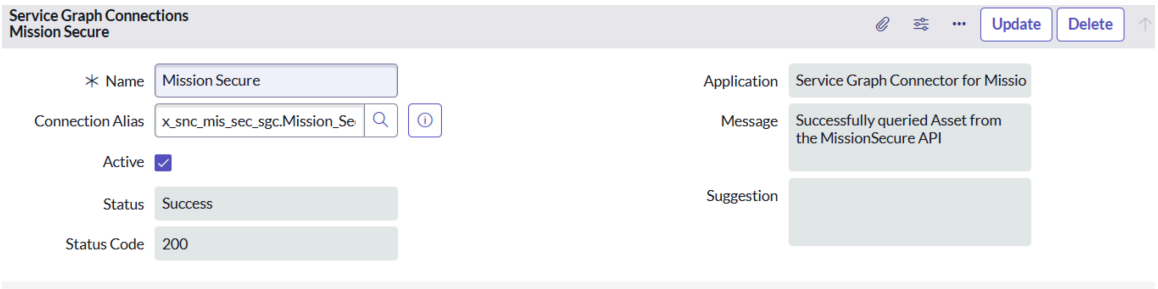
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Support and troubleshooting

Common troubleshooting options when you set up the integration for the Service Graph Connector for ServiceNow OT Discovery.

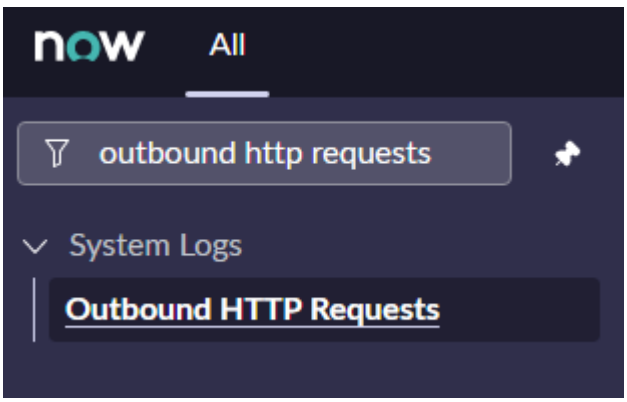
Test the connection

You can test the connection after configuring your URL and credentials for the integration. If everything is configured correctly, the service graph connection displays a successful connection test without any error. If something goes wrong during the connection, the Service Graph connection displays the error message, error code, and response body from the API.

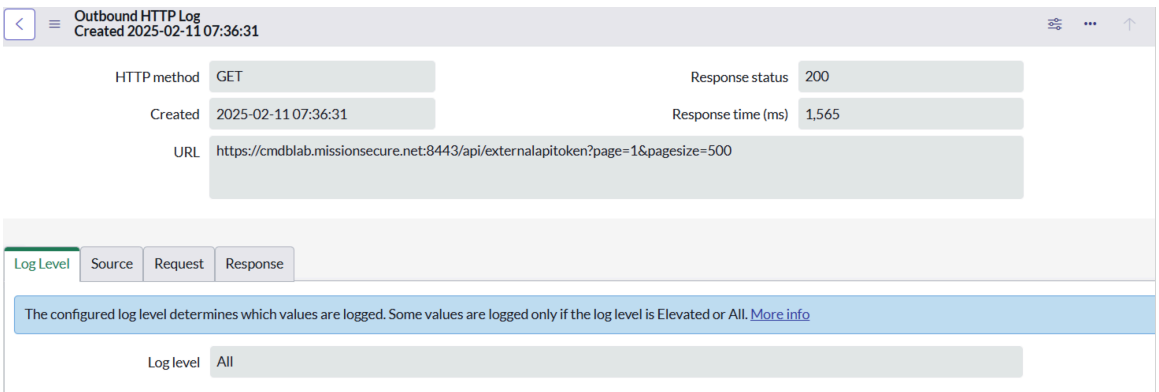


Review Outbound HTTP Request records

You can also review the Outbound HTTP Request records associated with the test. Navigate to **All** > **System Logs** > **Outbound HTTP Requests**.



In the list view, you should see the URL hostname that you specified when setting up the connection parameters. Open this record to view the connection details.



By default, the log level is set to Basic, so you can't see the response body or quest body, but the response status indicates the issue. For example, a 401 in the Response status indicates an unauthorized request. To resolve the issue, navigate to the connection and verify that you have

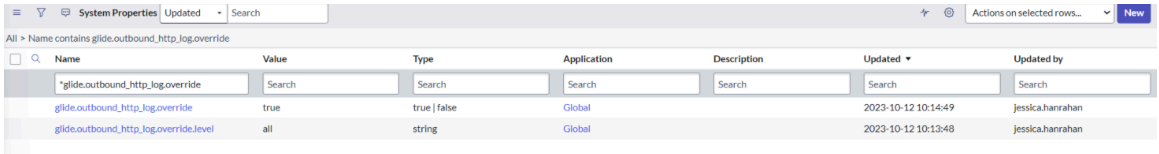
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the correct Client ID and Client Secret entered for the connection. For more information, see Install the Service Graph Connector for ServiceNow OT Discovery Service Graph Connector for ServiceNow.

Additional diagnosis

If you must diagnose further, you can override the log level to give more information, for example using the global system properties. Navigate to the system properties by going to **sys_properties.list** in the application navigator and update the **glide.outbound_http_log.override** to the value true and update the **glide.outbound_http_log.override.level** to an appropriate value. For example, change value to **All**.

Note: You can perform action only for a limited period of time for troubleshooting. Make sure you revert the changes to the original configuration.



With extended logging turned on, you can provide additional details for requests after that to give more context to the issue.

If you encounter a response status of 401, it's typically an issue with your credentials. To resolve, navigate to the connection in the Flow Designer and verify that the API Key is filled in as expected with the correct value.

If you encounter any issues with the flattening of the Asset or missing data from the API, you can run a test load and validate the flattened data from the Staging table. Then compare it with the **api_data** to see if the data was provided from the API.

SGC Central

Use SGC Central to set up your Service Graph Connector for ServiceNow OT Discovery, then import data from your OT Discovery environment into your ServiceNow instance.

SGC Central is recommended for setting up the Service Graph Connector for ServiceNow OT Discovery. It simplifies connector deployment with intuitive setup options and step-by-step playbook guidance. Alternatively, you can use the original Guided Setup. See Service Graph Connector for ServiceNow OT Discovery Guided Setup.

SGC Central is available as a view in the CMDB Workspace or can be searched for in the **All** menu. The application enables you to discover and install Service Graph Connectors, and then effectively manage the full life cycle of creating, editing, monitoring, and debugging connections. The SGC Central application also verifies that connectors remain supported and up-to-date with certified partners.

Use the links in the Related Topics section to learn more about SGC Central.

SGC Central prerequisites

Get started with SGC Central and set up the prerequisites for the Service Graph Connector for ServiceNow OT Discovery

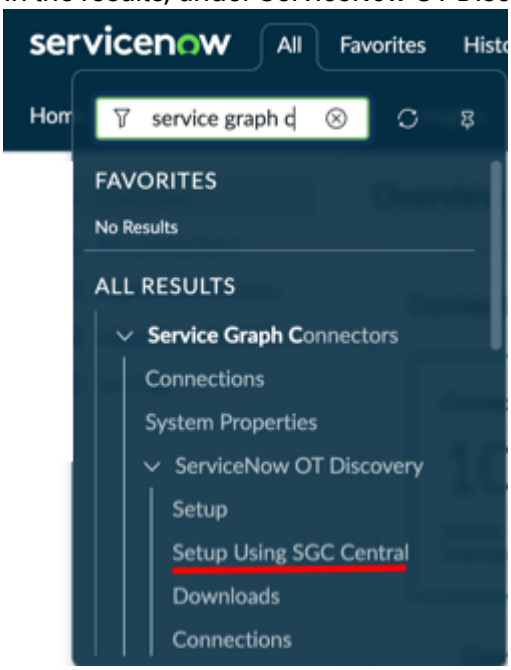
Before you begin

Role required: admin

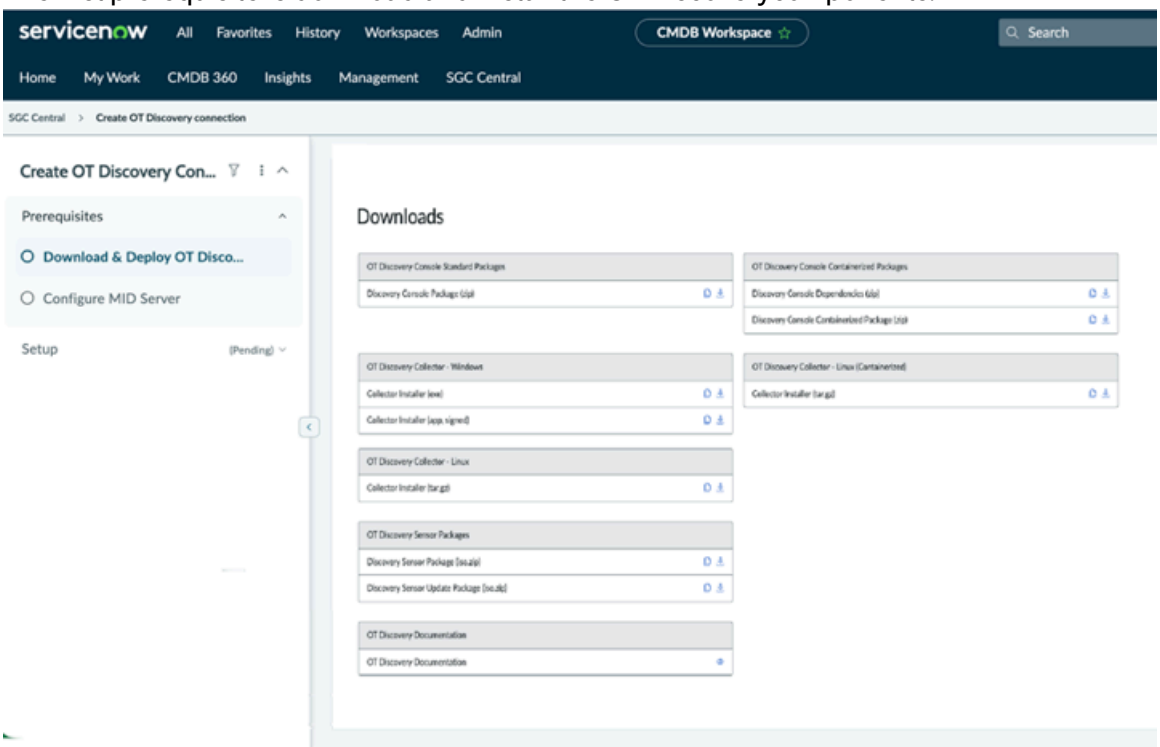
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to the **All** menu and type in search field **service graph connector**.
   You can also access SGC Central by navigating to the CMDB Workspace.
2. In the results, under ServiceNow OT Discovery, the **Setup Using SGC Central** option displays.



3. Select the **SGC Central** tab.
4. There are two prerequisites you much complete before you can create connections for the Service Graph Connector for ServiceNow OT Discovery:
5. The first prerequisite is download and install the OT Discoverycomponents.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

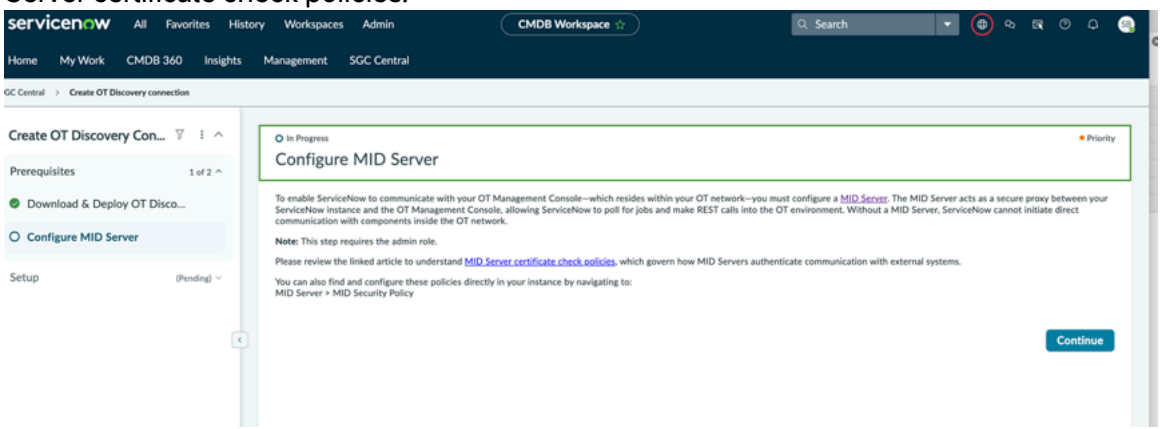
a. Download and install the Discovery Console for OT package.

b. Download and install the Discovery Sensor for OT package (ISO and OVR).

c. Download and install the OT Discovery Collector package that's compatible with your OS.

Note: You can download and install the Console and Collector containerized packages. Be sure to select the Collector package that is compatible to your OS. For more information, see Air-gapped networks and OT Discovery installation.

6. The second prerequisite is to configure the MID Server.
Configure the MID Server using the MID Server Guided Setup. Select the link to review the MID Server certificate check policies.



7. Verify that the prerequisites are complete and select **Continue**.

Configure and test connections

The SGC Central playbook launches when you start to configure and test connection.

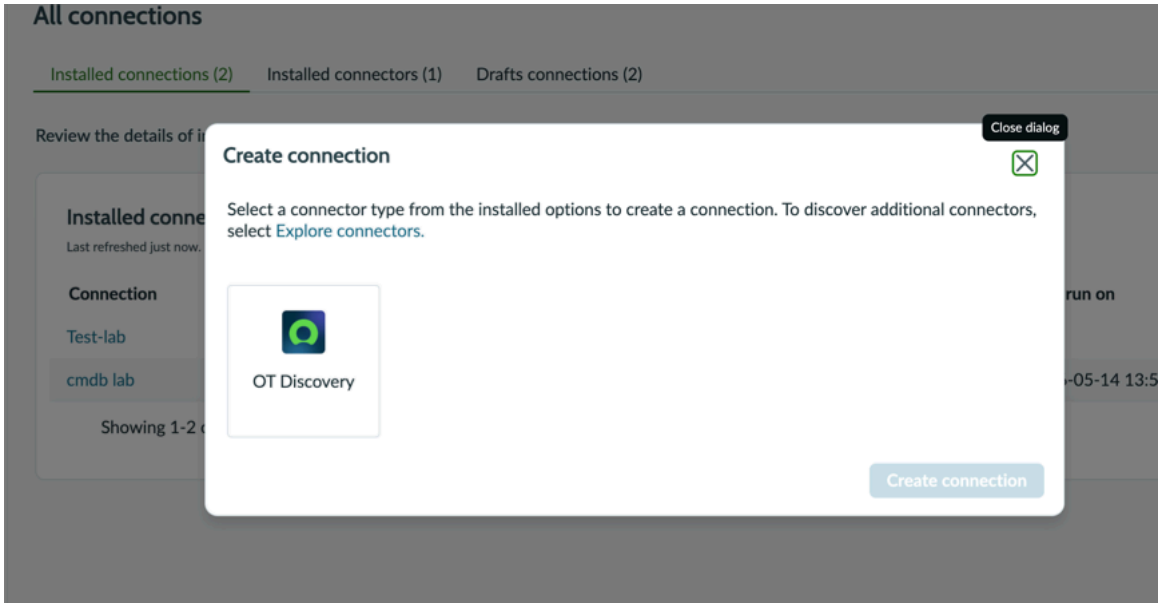
Before you begin

Role required: admin

Procedure

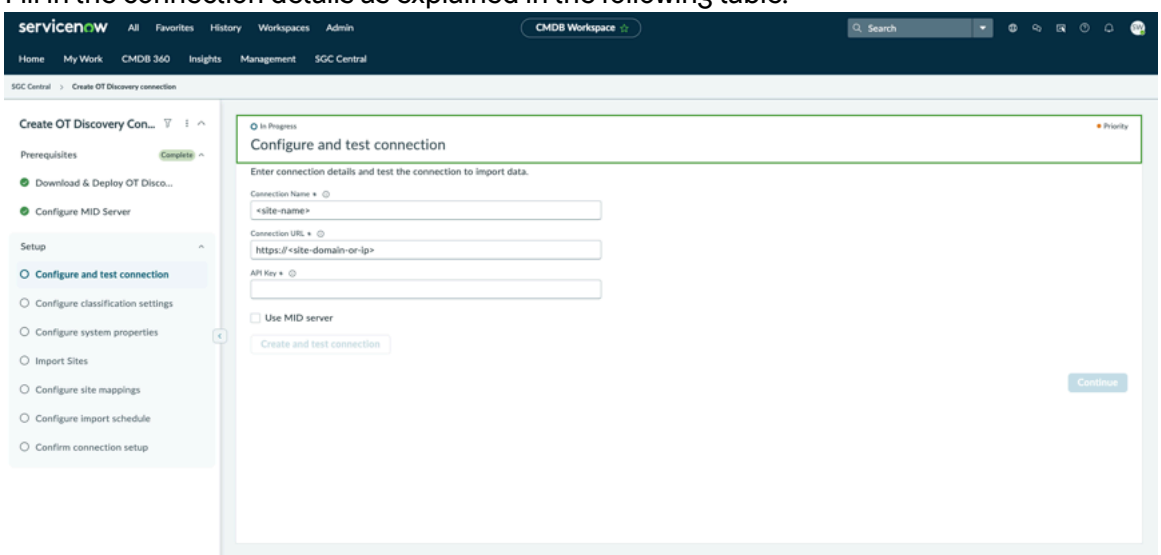
1. From the **Setup** section, select **Configure and test connections**.
After you select the **Create connection** button, a guided playbook experience launches automatically. The playbook walks you through each required configuration step for the Operational Technology Discovery connector.
2. Select the **Create connection** button.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The **Create connection** window opens.

3. In the **Create connection** window, select **OT Discovery**.
4. Select the **Create connection** button in this window.
5. Fill in the connection details as explained in the following table.



Connection details

Field	Description
Connection Name	Enter a unique name for the connection. The default connection has the name as OT Discovery and is read-only. For additional connections, enter a unique name for each. This field is mandatory.
Connection URL	Navigate to the Discovery Console for OT and copy its URL and paste it into the Connection URL field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	For example: https://OTDiscoveryConsole.net:8443/ This field is mandatory.
API Key	To get the API Key: **a.** Go to your Console and navigate to the **Settings** page. **b.** Open the **API** tab and select the Add icon. **c.** In the **Generate API Token** window, select the expiration length you want and select **Generate Token**. **d.** The generated token is listed in the Active token list. **e.** Select the Copy icon to copy the token. **f.** Paste the token key into the **API Key** field. **g.** Select **Save**. This field is mandatory.
Use MID Server	This is optional. Check this box to use a MID Server for the connection.

6. Select the **Create and test connection** button.
7. If successful, you see the **Connections verified** banner.
8. Select **Continue** to move to the next step.

Configure classification settings in SGC Central

In SGC Central, you can configure the Service Graph Connector for ServiceNow OT Discovery classifications settings to define how OT Discovery categories are mapped to the CMDB classes.

Before you begin

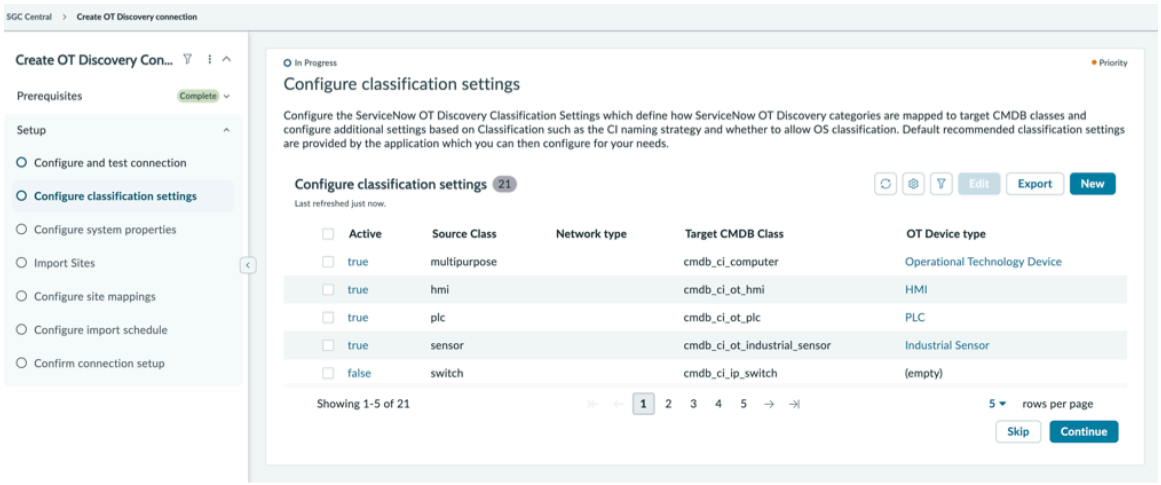
Role required: admin

Procedure

1. When you select Continue in the Configure and test connections step, the Configure classification settings step opens.
2. Review the classification settings.

> **Note:** The OT Discovery classification settings define how OT Discovery categories are mapped to the target ServiceNow Instance CMDB classes. It also defines how they are configured to additional settings based on classification, such as the configuration item (CI) naming strategy and whether to permit OS classification. The default recommended classification settings are provided by the application, which you can then configure for your needs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. In this step, you can edit, export, or create settings.
   You can select **Skip** to skip this step.
4. All the devices that are imported follow a default naming strategy.
5. You have the flexibility at a class level to change the name.
6. You can map the Target CMDG Class name to an OT Device type and can change the mapping settings.
7. If any changes are needed, select the OT Device Type, open the classification settings record, and update the entries in the following fields:

OT Discovery Classification Setting fields

Field	Description
Active	True. If checked, the Classification Setting is used when classifying the devices. If unchecked, the Classification Setting is ignored.
Source Class	The class name of the source asset.
Network type	Defines whether this classification setting is for OT or IT devices only. Leave empty to include both types. If OT devices with a specific category must be classified into a separate class from IT devices, there are two definitions for the OT Discovery Category. One definition has the Network type set to **OT** with the classification for the OT devices. The other definition is set to **IT** for classifying the IT devices.
Target CMDB class	The CMDB class to target when importing the OT Discovery device.
OT device type	For OT devices, you can select the OT device type to apply the device type to the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	imported OT Discovery devices in the CMDB, if applicable.

8. Select **Continue** to move to the next step.

Configure system properties on SGC Central

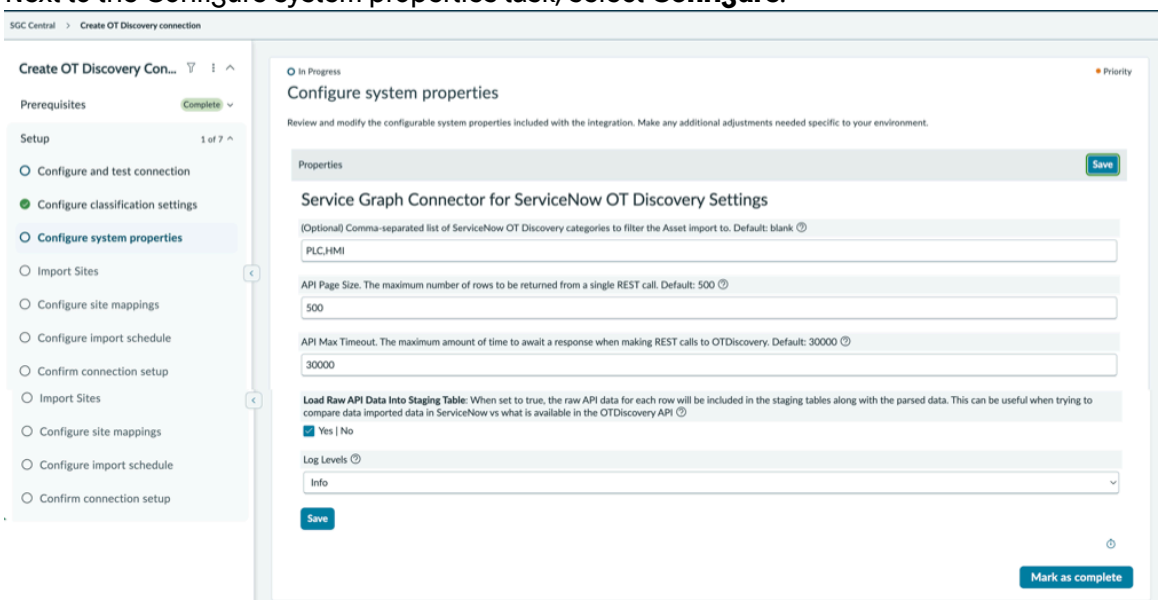
In this step, review and modify the configurable system properties included with the integration.

Before you begin
Role required: admin

Procedure

Next, review and modify **Configure system properties** included in the integration.

a. Next to the Configure system properties task, select **Configure**.



b. The Configure System properties window opens.

c. Review the System properties and adjust as needed for your instance configuration.

System properties

System property	Description
(Optional) Comma-separated list of OT Discovery categories to filter the Asset imports.	Filters the Asset import to only import assets of particular categories. For example, if you wanted to only import ICS Host and PLC category devices from the Discovery Console for OT, you could set this to `PLC,IcsHost`. Default: empty **Note:** These are categories defined on the Console side.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System property	Description
API Page Size	Maximum number of rows to be returned from a single REST call. Default: 500
API Max Timeout	Maximum amount of time to wait for a response when making REST calls to OT Discovery. Default: 30000
Load Raw API Data into Staging Table	When set to true, the raw API data for each row is included in the staging tables along with the parsed data. This is useful when trying to compare data imported data into ServiceNow vs. What is available in the OT Discovery API.
Log Levels	Logging level verbosity to use for the application. Default: Info

d. Select **Save** and move to the next step.

Import Sites

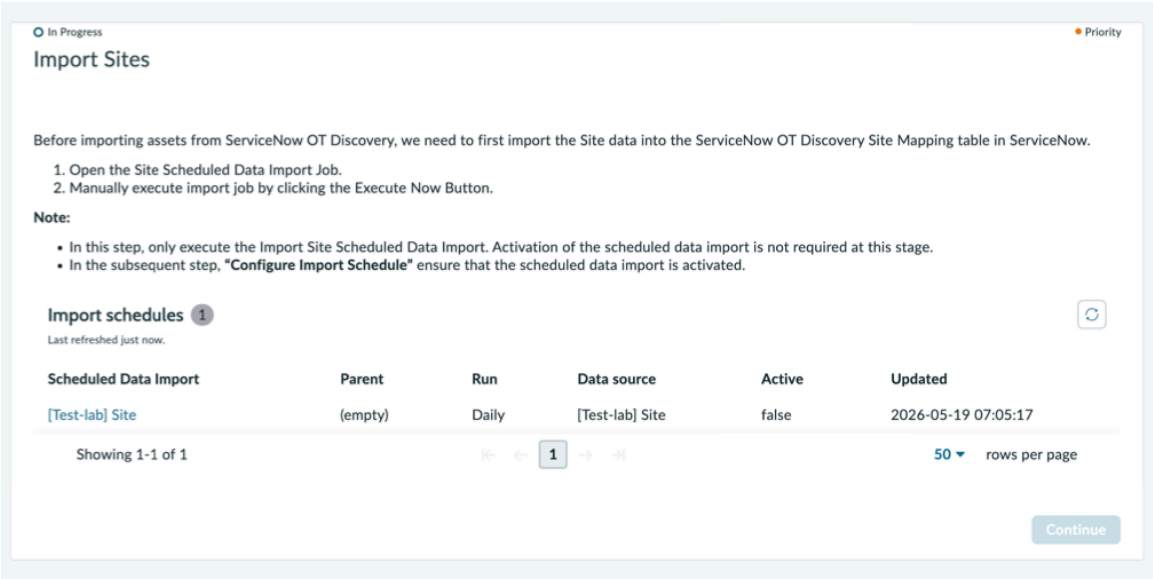
In SGC Central the next step is to import the Sites.

Before you begin

Role required: admin

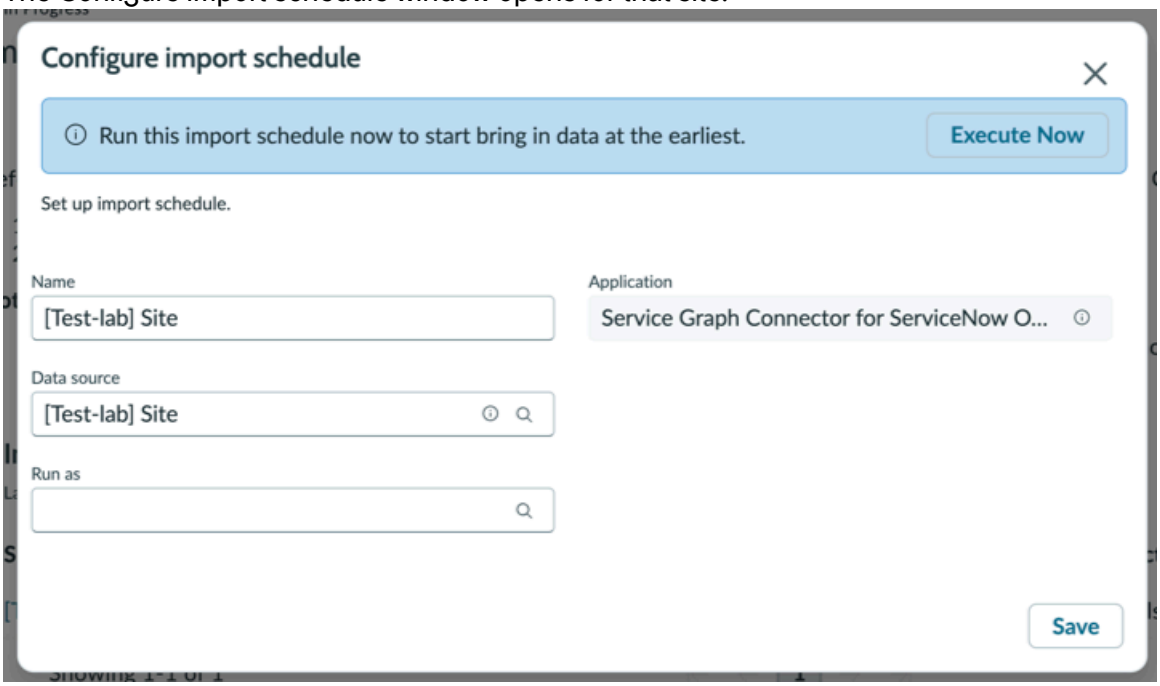
Procedure

1. In the SGC Central setup process, you must import sites before importing assets.

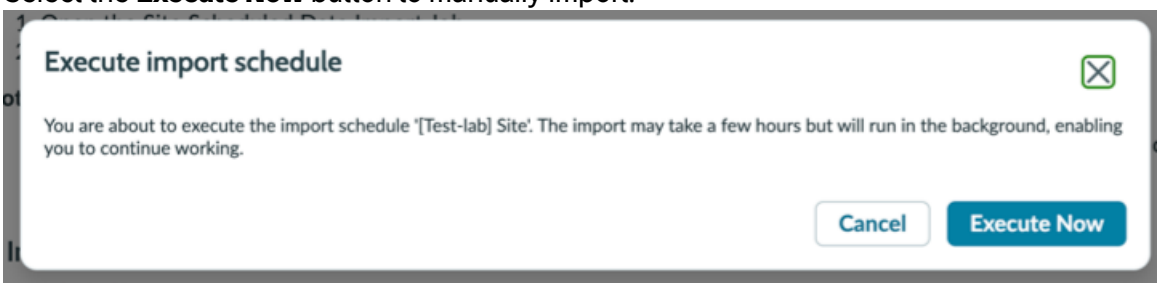


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Open the **Site Scheduled Data Import** job; that is, select the site displayed under **Scheduled Data Import**.
3. The Configure import schedule window opens for that site.



4. Select the **Execute Now** button to manually import.



5. Repeat these steps for additional sites.
6. Select **Continue** to move to the next step.

Configure site mappings

Importing the site data must be complete before you can move onto configure site mappings.

About this task

Before proceeding, review and configure imported ServiceNow OT Discovery site mapping records and verify that the site data has been fully imported via the site scheduled data import. The site mapping records will not be available unit the import is complete.

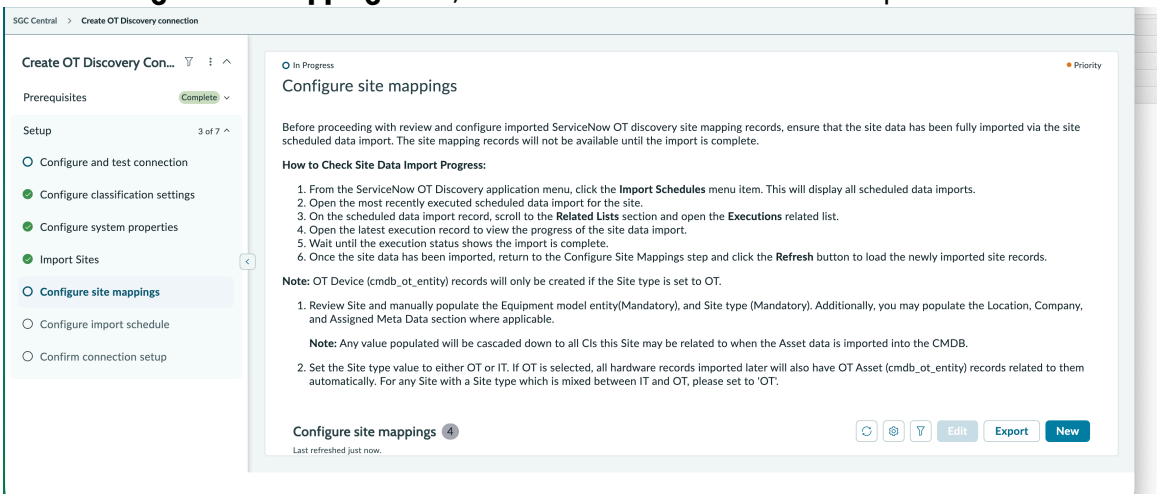
Before you begin

Role required: admin

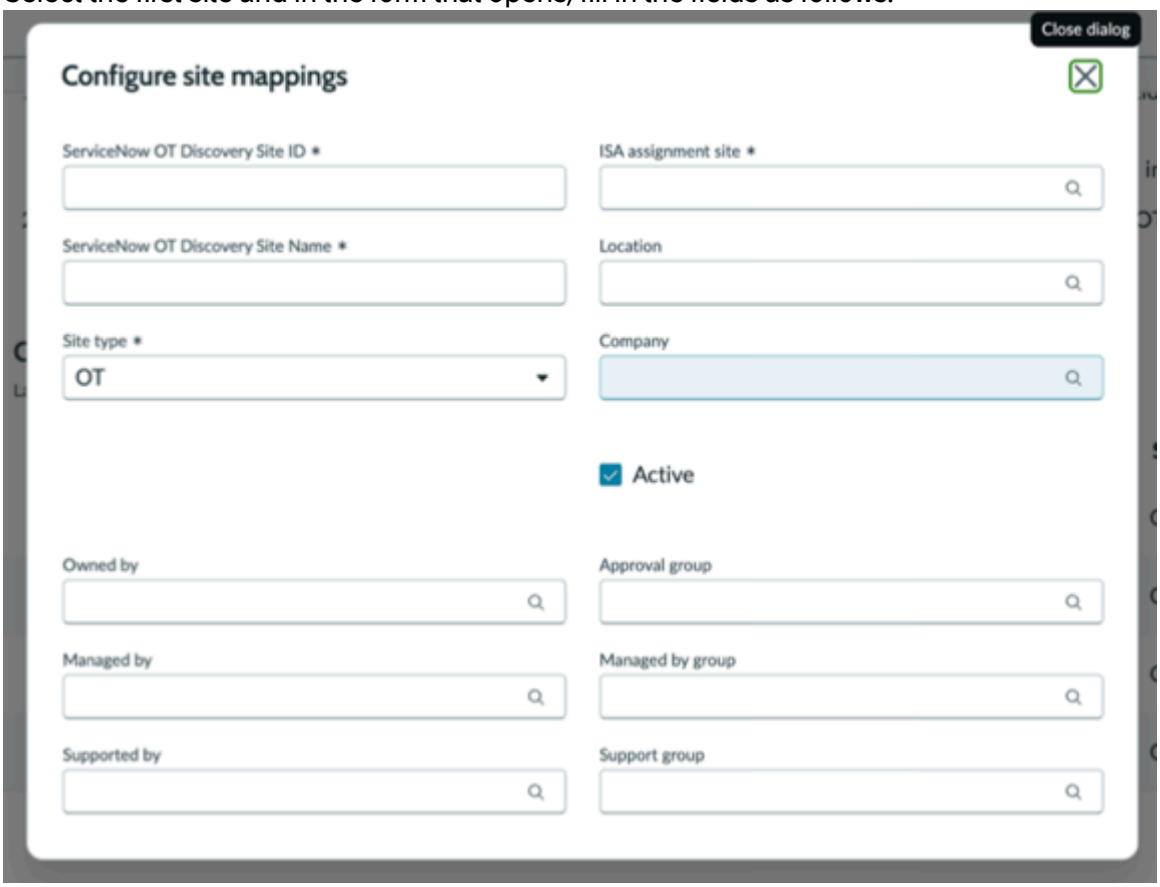
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. In the **Configure site mappings** task, scroll down to review the list of imported sites.



2. Select the first site and in the form that opens, fill in the fields as follows.



   a. All field titles with * (asterick) next to them are mandatory and should be filled in.

   b. Select a value in the **Site type** field.
   The value can be either **OT** or **IT**. If you select **OT**, all hardware records imported later also have OT device (*cmdb_ot_entity*) records related to them automatically. For any site with a site type between IT and OT, select **OT**.

   c. Select an **ISA assignment site**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

All data in the site imports to the ISA assignment site you select.

d. If applicable, populate the **Location** and **Company** fields.

e. Check the **Active** box.

Note: Any value populated is cascaded down to all configuration items (CIs) this Site is related to when the asset data is imported into the CMDB.

3. Select **Continue** to move to the next step.

Create import schedule

After importing sites and configuring site mappings, you can create an import schedule.

Before you begin

Role required: admin

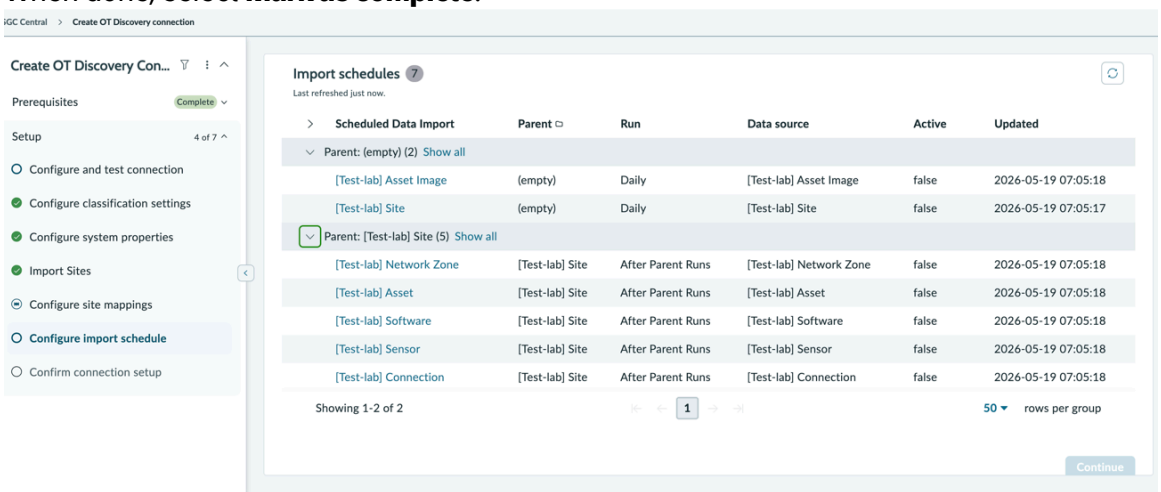
Procedure

1. Do the **Configure scheduled jobs** task next.
By default, the ServiceNow OT Discovery scheduled jobs created during installation are inactive. All other jobs are configured to run after their parent job, the Site Scheduled Data Import Job. The only exception is the Asset Image import jobs, which run independently.

The following schedules jobs are available to import data:

- **Asset import**: This imports the OT Devices discovered into CMDB.
- **Network Zone import**: This imports the list of Managed Networks defined within the Site to support the deployment of OT Discovery.
- **Sensor import**: This imports list of all the Sensors used for OT Discovery deployment into the NIDS table.
- **Connection import**: This imports the list of communications between the devices.
- **Asset Images**: This imports the list of screenshots captured during the discovery process in the cmn_media table.

2. When done, select **Mark as complete**.

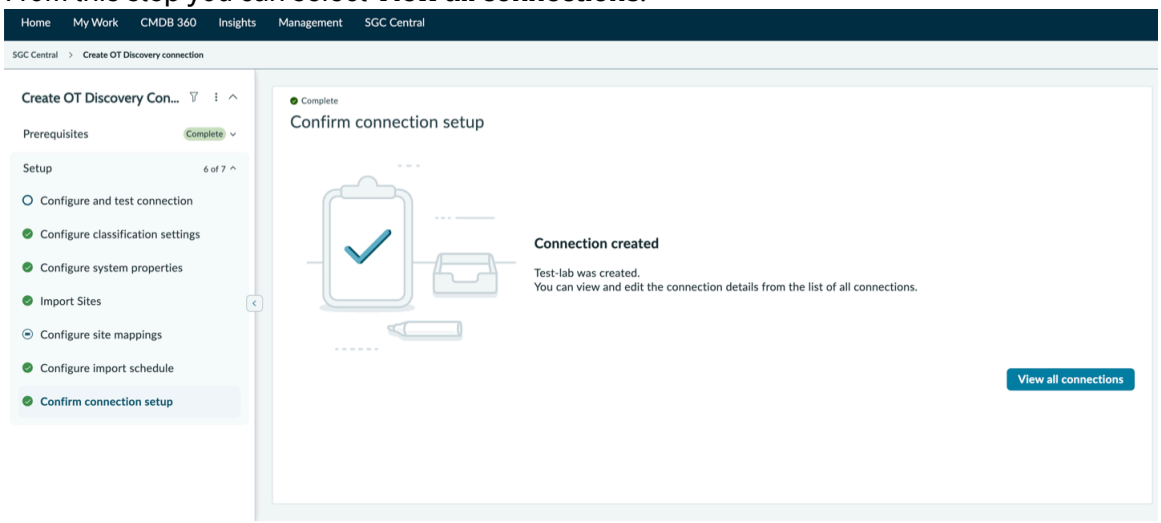


3. Navigate to **Confirm connection setup**.

4. Check the connection setup to confirm it is valid.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. From this step you can select **View all connections**.



Review imports

This section reviews all your importation settings in SGC Central.

About this task

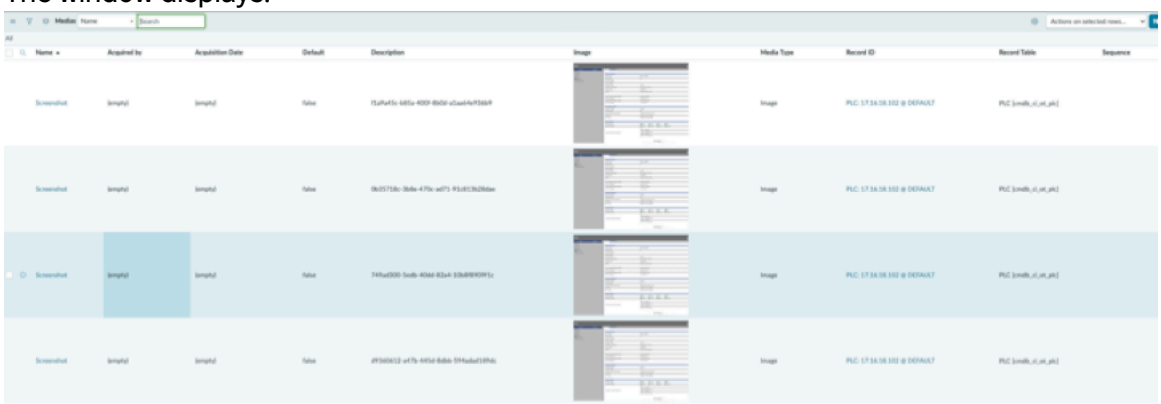
After you have completed the steps of the SGC Central OT Discovery playbook, you can review your imports by following this process.

Before you begin

Role required: admin

Procedure

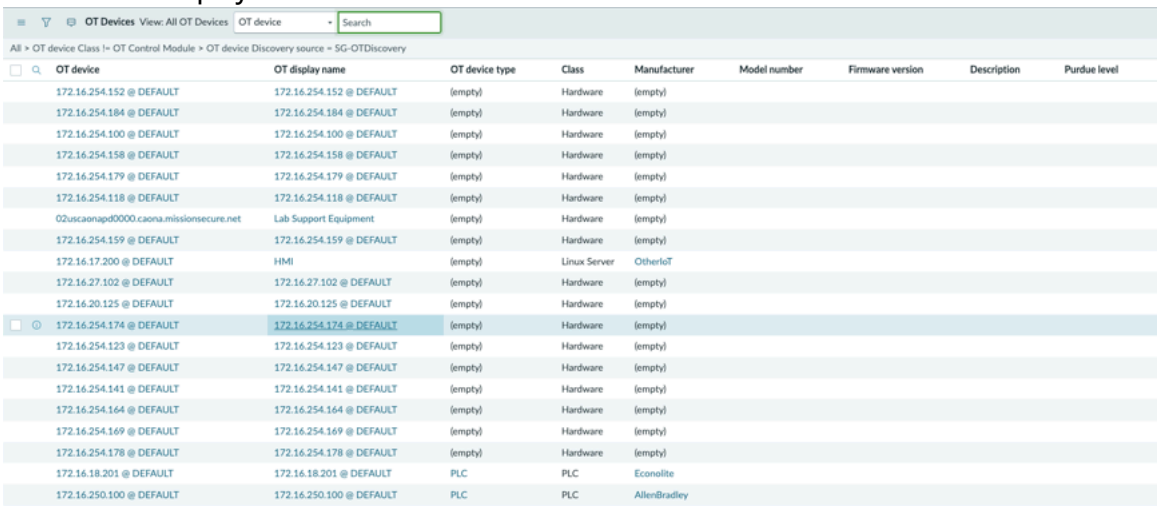
1. Navigate to the **All** menu and type in "discovery" in the search field.
2. From the drop-down list, choose a review task.
   After completing the configurations and scheduling imports in the SGC Central, you can now go back and review the settings. Select:
   - Review Imported OT Devices
   - Review Imported Network Connections
   - Review Imported Images
3. For example, select **Review Imported Images**.
   The window displays:



4. Select **Review Imported OT Devices**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The window displays:



Feedback on OT Discovery

To provide feedback on OT Discovery you can submit a NOW idea on ServiceNow support.

Now idea

- To open a NOW idea, log in to the support portal. When filling out the form, set the "Title" field to "Feedback on OT Discovery" and set the Product field to "Operational Technology Manager".
- When sharing data related to unknown devices (that is, devices that were not accurately identified/classified), provide additional information related to manufacturer, brand, product model, and version.
- DO NOT share any sensitive or confidential information, including proprietary information or data specific to a customer or user, such as IP addresses, user information, or passwords when submitting this form.

Note: To find the **Feedback on OT Discovery** page, enter "OT Discovery" in the **All** menu in your instance or navigate directly to the Create an Idea form: https://support.servicenow.com/now?id=create_edit_idea&sysparm_module_id=enhancement_requests.

IT Discovery for Operational Technology (OT) Networks

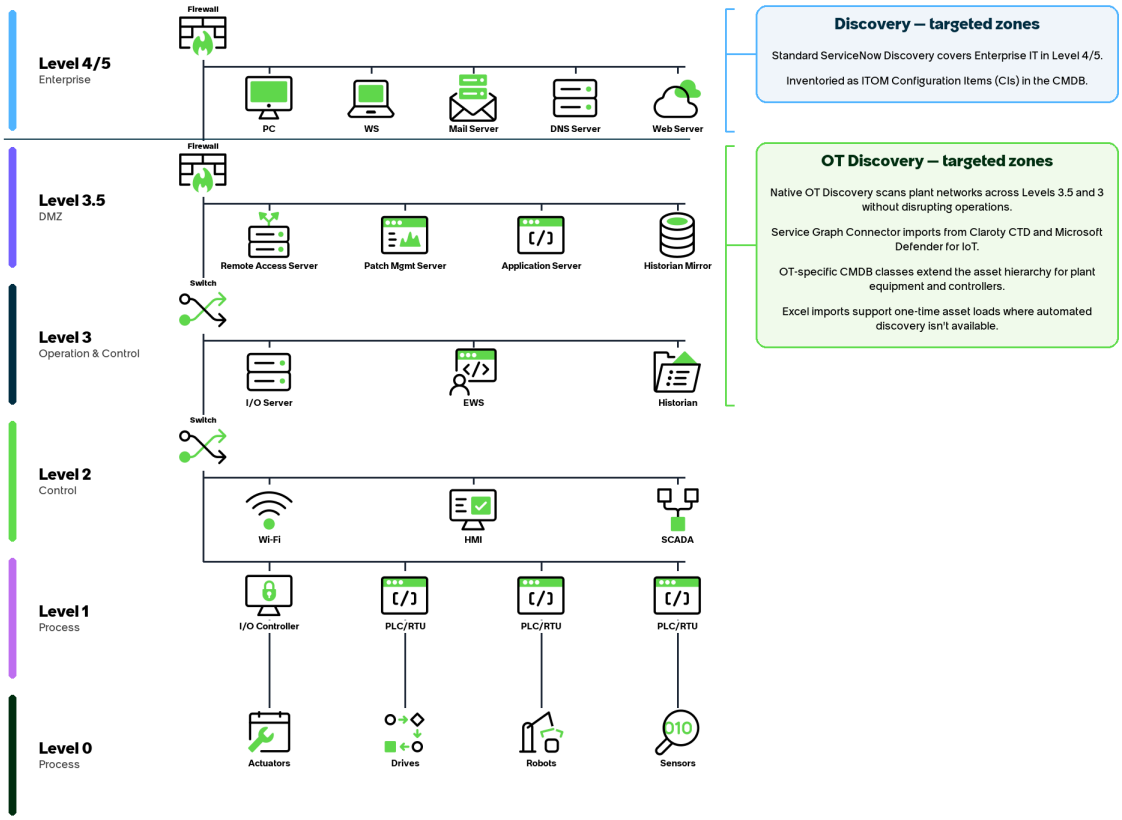
You can use the IT Discovery for Operational Technology (OT) Networks function to discover IT class OT devices. These devices are located in designated Purdue levels within your Industrial Control System (ICS) networks. IT class items include switches, routers, and computers that exist both in data centers and in your factories.

Where standard Discovery processing takes place

The IT Discovery for OT Networks process operates in a manner that is similar to the standard Discovery processes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Targeted Purdue levels in standard and IT Discovery for OT Networks Discovery



Standard Discovery processing in the ServiceNow AI Platform® normally takes place in the following Purdue levels in your enterprise:

Processed Purdue levels

Purdue Level	Description
4	Site business and logistics, such as all Information Technology (IT) functions.
5	Enterprise Network, where Enterprise Resource Planning (ERP) functions take place.

Note: To learn more about Purdue levels in Industrial Control Systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.

Where and how IT Discovery for OT Networks processing takes place

In contrast, IT Discovery for OT Networks processing can take place in the following Purdue levels, depending on which you select when you create an OT discovery schedule:

Processed Purdue levels

Purdue Level	Description
3.5	Demilitarized Zone (DMZ) or Industrial Demilitarized Zone (IDMZ). Similar to a traditional (IT) DMZ, the OT-oriented IDMZ

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

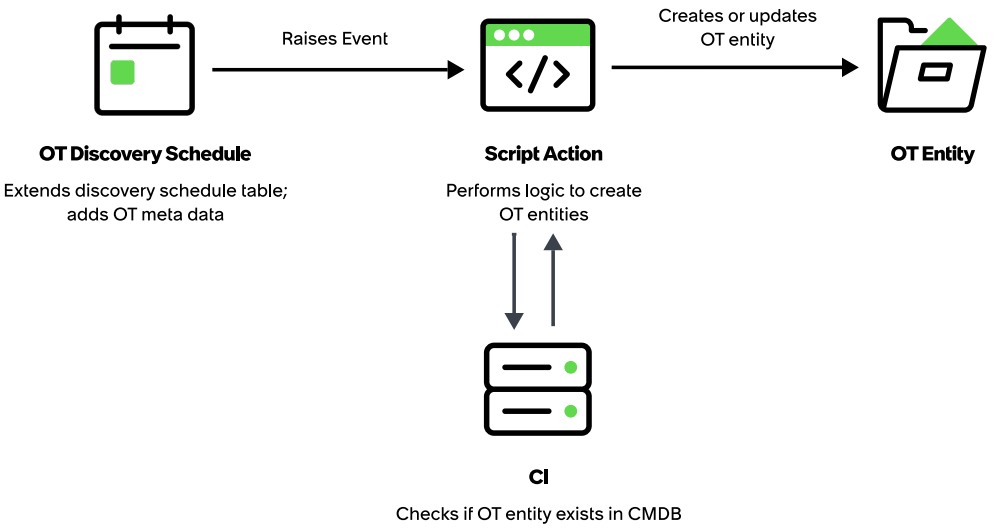
Processed Purdue levels (continued)

Purdue Level	Description
	enables you to securely connect networks with different security requirements.
3	Site operations where plant or site-wide control and monitoring functions reside.

You typically run IT Discovery for OT Networks in the DMZ (or IDMZ, Purdue Level 3.5) of your ICS networks. This Purdue level is where there are usually IT and OT class computers and servers to discover and manage.

Note: To avoid the possibility of disrupting your industrial operations, you should not run Discovery processes against Purdue levels 0 through 2 in your ICS networks.

IT Discovery for OT Networks processing



When you run an OT Discovery schedule, it performs the following processing:

1. Proceeds through the assigned IP addresses and discovers all hardware items that exist in it.
2. When it completes Discovery of a configuration item (CI), it internally triggers a (discovery.device.complete) event. This logic checks if an OT entity (cmdb_ot_entity) record exists for it in the Configuration Management Database (CMDB).
   - If one exists, and any related attributes have changed for the discovered item, it updates the OT Entities that are related to that CI.
   - If one does not exist, it creates one for it.
3. In addition to the location attribute, it also pushes the defined attributes from the OT Discovery schedule to the CI and to the related OT entity records.
4. It also creates OT entity records for the applications installed on discovered OT devices. To view the applications that have OT entity records created through IT Discovery for OT Networks, navigate to the Industrial Workspace list view and open the **Applications** list under *Operational Technology* **(OT)**.

Note: For more information about the Operational Technology Discovery solution, see Operational Technology Discovery.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IT Discovery for OT Networks related links and lists

IT Discovery for OT Networks contains several related links and lists.

Related links

Related link	Description
Quick Ranges	IP addresses and address ranges to scan when the OT discovery schedule runs. Enter IP addresses in multiple formats (network, range, or list) in a single, comma-delimited string. The MID Server in use must be able to connect to the specified IP ranges. For more information, see Create a Quick IP range for a Discovery schedule.
Discovery now	Run the IT Discovery for OT Networks process immediately.
Run Point Scan	Access to the Execute Point Scan dialog. To learn more, see Execute a point scan.

Related lists

Related list	Description
Discovery IP Ranges	Discovery IP addresses and address ranges to scan and discover. If you're using a simple CI scan (no behaviors), use this related list to define these IP addresses. The MID Server in use must be able to connect to the specified IP ranges. **Note:** To improve security, limit the range of Discovery targets to exclude unnecessary networks and devices.
Discovery Range Sets	Definition of each range set that the OT Discovery schedule scans, using one or more Shazzam probes.
Discovery Status	History of the results of the current and past OT Discovery schedule runs.

Related topics

- MID Server
- Shazzam probe, port probes, and protocols
- Create a Shazzam probe

Create and run the OT Discovery schedule and the Discovery process

Define Operational Technology (OT) Discovery schedules that orche schedules that orchestrate how and when the Discovery strate how and when the Discovery for an OT function should run. You can also perform an immediate Quick Discovery or an actual OT Discovery run.

Before you begin

Do the following actions before you run IT Discovery for OT Networks:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Install and configure the standard Discovery application. To learn more, see Discovery setup.
- Install the CMDB CI Class Models plugin. To learn more, see Operational Technology (OT) extension classes installation.
- Install the Mid Server. To learn more, see Installing the MID Server.

Role required: ot_discovery_admin

Procedure

1. Navigate to **All** > **OT Discovery** > **OT Discovery Schedules**.
2. Run Quick Discovery or select or create an OT Discovery schedule.

Task	Description
Run an immediate Quick Discovery	Select **Quick Discovery** and do the following actions: **a.** In the **Target IP** field, enter the IP address in which the Discovery for the OT process should run. **b.** In the **MID Server** field, select the MID Server in which the Discovery process should run. **c.** Select **OK**.
Select or create an OT Discovery schedule	**a.** Select an existing OT Discovery schedule or select **New** to create a new schedule. **b.** Perform the steps that follow to create the OT discovery schedule record in the OT Discovery Schedule form.

3. In the form, fill in the OT Discovery Schedule fields.

Field	Description
Name	Unique, descriptive name for your OT Discovery schedule.
Discover	Scan type for the OT discovery schedule. **Configuration items** Uses Discovery identifiers to match devices with configuration items (CIs) in the CMDB and to update the CMDB. Perform a simple discovery by selecting a specific MID Server to scan for all protocols (SSH, WMI, and SNMP) or perform advanced discoveries with discovery behaviors. When you select a behavior, the *MID Server* field is not available. **IP addresses**

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Scans devices without the use of credentials. These scans dis cover all the active IP address es in the specified range and cre ate device history records, but do not update the CMDB. IP ad dress scans also show multiple IP addresses that are running on a single device. Identify devices by class and by type, such as Windows computers and Cisco network gear.
Default Purdue level	Purdue level that you want the OT discovery schedule to run in or select **--None--** for all Purdue levels. **Note:** To learn more about Pur due levels, see https://subscrip tion.packtpub.com/book/network ing_and_servers/9781788395151/ 1/ch01lvl1sec10/the-purdue-model-for-in

Most of the fields on this form are identical to or operate in the same manner as the standard Discovery form. Only those fields that differ from the standard Discovery scheduling appear in this topic. To learn more about the remaining fields, see Schedule a horizontal discovery

4. Run the Discovery process right away, or save the OT discovery schedule to run at the times you designated in the record.

Task	Description
Run Discovery immediately	Select the **Discover now** related link.
Run Discovery at the time designated in the OT discovery schedule	Select **Update**.

Result
When the IT Discovery for OT Networks process runs, it creates a history record in the Discovery Status related list.

Industrial Process Manager

Use the Industrial Process Manager application to create the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Operational Technology solution. The Industrial Process Manager enables you to create your own version of the equipment models in each of your sites.

Note: The Manufacturing Process Manager was renamed to the Industrial Process Manager for Vancouver. If you're on version 1.0.9 and prior, the application is still called Manufacturing Process Manager. If you're on version 2.0, the application is called Industrial Process Manager.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Watch an overview about the Industrial Process Manager application.

https://player.vimeo.com/video/1044353688?h=eba3593d47&badge=0&autopause=0&player_id=0&app_id=58479

Explore	Configure
 Learn about how manufacturers use the Industrial Process Manager	 Plan and configure your implementation
Use	**Reference**
 Review Operational Technology devices and equipment model entities	 Get details about related information and applications

Explore Industrial Process Manager

Learn more about the common terminology, acronyms, and ISA-95 Equipment Model industry standard used in the Industrial Process Manager.

Industrial Process Manager common terminology

Before getting started with the Industrial Process Manager, here are some common terminology and acronyms.

Common terminology and acronyms

Term	Acronym	Definition
Operational Technology	OT	Technology that is used for industrial automation to control physical processes. **Note:** Operational Technology is not the Internet of Things (IoT).
International Society of Automation	ISA	Organization that publishes the standards for industrial enterprises, including the ISA-95 equipment model.
Extract, Transform, Load	ETL	Common term that is used for taking data from a source system, transforming it, and then uploading it to a target system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ISA-95 equipment model

The ISA-95 equipment model is an industry standard that represents an industrial facility and the production equipment in it. Describe the equipment model entities in your facilities by defining an equipment model template with different levels and level types.

With this template, you can:

- Map your equipment model entities. With this map, you create a hierarchical structure.
- Create multiple equipment models for multiple industrial sites.
- Assign users to each site so that you can manage their access to the equipment model information for specific sites. For example, you can designate that users in Atlanta can access only the Atlanta site information but not the data for a site in Michigan. To learn more, see Manage equipment model site access for non-administrators.

The equipment models start at the site level and contain a detailed hierarchical structure that describes each industrial site. You can apply an equipment model template to structure this data in a hierarchical sequence.

Equipment model entity records are located in the Equipment Model Entity [cmdb_ci_ot_isa_entity] table. For more information about managing your equipment model entity, see Managing equipment models.

The following graphic shows the standard ISA-95 default template delivered when you install the Industrial Process Manager.

- The subordinate levels under a site represent the door assembly area, its own subordinate work centers, and work units.

  A work cell is a designated area within a manufacturing facility where a group of resources are strategically arranged to work together and complete a specific task or process efficiently. A work center includes people, machinery, and equipment.

- The Work Centers and Work Unit levels each have level types. In this model, there are four different level types for the Work Center level:
  - Process Cell: An area within a manufacturing facility dedicated toward a particular stage of production. It includes all necessary equipment such as programmable logical controllers (PLCs), sensors, and actuators to automate and monitor processes. Process cell data is collected for control, quality monitoring, and diagnostics.

    For example, a robotic welding cell in an automotive factory.

  - Production Unit: A group of process cells that perform related manufacturing operations. It coordinates process cell activities and manages material and data flow.

    For example, a car manufacturing plant production unit might include cells for welding, painting, assembling, and packaging.

  - Production Line: A sequence of process cells or production units that manufacture a product from start to finish. It provides overall control and monitoring, and coordinates activities across all cells and units. It also manages the entire process from raw materials to finished goods.

    For example, an automotive assembly line where parts are assembled into a complete vehicle.

  - Storage Zone: A designated area for storing raw materials, work-in-progress items, or finished goods. Inventory management systems maintain material flow and availability.

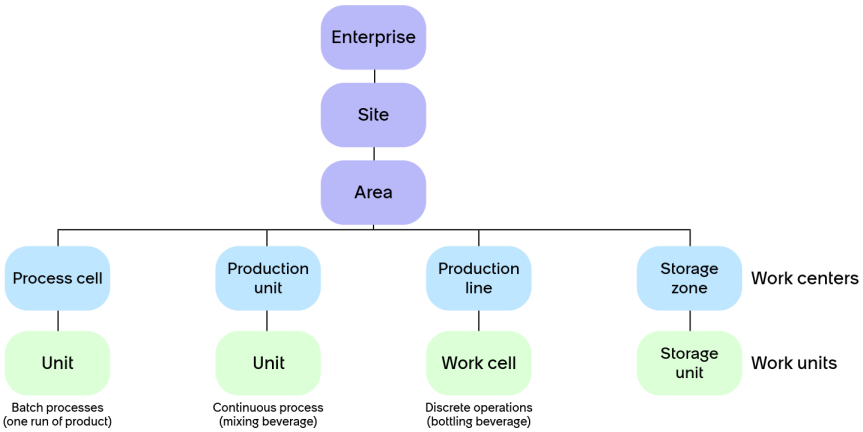
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, a warehouse for raw materials before production or finished goods awaiting shipment.

- Storage Unit: A designated space or structure for keeping specific equipment, materials, or products.

  For example, a car manufacturing plant uses storage units for car paint, electrical accessories, and raw steel.

Equipment model template example



Equipment model templates

Create equipment model templates to characterize equipment models or organize data by grouping similar entities.

An equipment model template consists of the following components:

Equipment model template

Name and description of the equipment model template.

Equipment model template hierarchical levels

Assigned hierarchical levels that are used to sort and structure the equipment model data.

Equipment model template hierarchical level types

Types that represent different types of the areas, functions, or production processes within a hierarchical level.

To learn more about equipment templates and see a graphic example of their structure, see ISA-95 equipment model and Defining equipment model templates.

Configure the Industrial Process Manager

Configure the Industrial Process Manager application so that you can create the Equipment Model data foundation that is required for the ServiceNow® Operational Technology solution.

Note:

If you have the admin role, you can use the Industrial Guided Setup to lead you through the setup of the Industrial Process Manager application.

To access the Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Purpose
1. Install the Industrial Process Manager from the ServiceNow Store.	Installs the Industrial Process Manager application and supporting plugins.
2. Assign Industrial Process Manager roles.	Assigns roles to control the actions that are available for each user.
3. Populate a Microsoft Excel spreadsheet for Service Graph Connector import.	Creates and populates a Microsoft Excel spreadsheet with your existing ISA-95 Equipment Model data for upload to the ServiceNow AI Platform.
4. Import your Excel spreadsheet.	Uploads your existing ISA-95 Equipment Model data to the Configuration Management Database (CMDB).
5. Install Service Graph[service-graph] connectors that are provided by ServiceNow® partners, and import the equipment model data using the integrations.	Installs ServiceNow connectors that are provided by partners as they become available in the ServiceNow® Store, and imports equipment model data.
6. Grant equipment model site access to users with non-administrative roles.	Assigns or removes site access for users with assigned cmdb_ot_isa_viewer or cmdb_ot_isa_editor roles.
Optional: Automate mapping of OT devices	Automates mapping of OT devices to the production process. **Note:** Enabling the mapping feature requires the following plugins: • Operational Technology Manager • Industrial Process Manager

Install the Industrial Process Manager

If you have the required entitlement and the Administrator [admin] role, you can install the Industrial Process Manager application and the related plugins.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.

Role required: admin

About this task

The following items are installed with the Industrial Process Manager:

- Plugins
- Application menu, including Guided Setup
- Roles
- Tables

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on viewing the components that are installed with the Industrial Process Manager application, see Components installed with Industrial Process Manager.

Note: For Operational Technology Service Management users with no license for Operational Technology Visibility, note the following:

- When you have the latest version of Operational Technology Incident Management installed, Industrial Process Manager is also installed.
- When you have the latest version of Operational Technology Change Management installed, Industrial Process Manager is also installed.

You should upgrade to the latest versions so you have access to the Operational Technology Service Management experience.

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Industrial Process Manager application by using the filter criteria and search bar.

   You can search for the application by its name or ID. If you can't find the application, you might have to request it from the ServiceNow Store.

   Visit the ServiceNow Store to view all the available apps, and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.
3. In the Application installation dialog box, review the application dependencies.

   Dependent plugins and applications appear if they will be installed, are currently installed, or must be installed. If any plugins or applications require installation, you must install them before you can install the Industrial Process Manager.
4. **Optional:** If demo data is available and you want to install it, select the **Load demo data** check box.
   Demo data are the sample records that describe application features for common use cases. Load the demo data when you first install the application on a development or test instance.
5. Select **Install**.

Industrial Workspace Admin application menu and Guided Setup

After you install the application and related plugins, you can use the Industrial Workspace Admin application menu to access the related Operational Technology Manager, Industrial Process Manager, Operational Technology Incident Management, Operational Technology Vulnerability Response, Operational Technology Change Management, Operational Technology Knowledge Management, and Operational Technology Request Management functions.

Industrial Workspace Admin application menu contents

To access the Industrial Workspace Admin application menu, enter `Industrial Workspace Admin` in the application navigator. The Operational Technology Management solution currently consists of the following applications and features:

- Operational Technology Manager
- Industrial Process Manager
- Operational Technology Vulnerability Response
- Operational Technology Incident Management

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Operational Technology Change Management
- Operational Technology Knowledge Management
- Operational Technology Request Management

Note: You need to install either the Operational Technology Manager or Industrial Process Manager applications first before using Operational Technology Incident Management and Operational Technology Change Management.

The options that appear on the Industrial Workspace Admin application menu depend on which OT applications are installed and what assigned roles the user has. When the Industrial Process Manager is installed, the following functions are available on the Industrial Workspace Admin application menu:

- Guided Setup
- All OT Properties
- Workspace System Properties
- OT Progress Scorecard Config
- OT Progress Scorecard Attributes
- OT Manager, which includes the following selections:
  - OT Manager Admin
  - Industrial Process Manager
  - OT Incident Admin
  - Operational Technology Change Management

To learn more about application installation and assigned roles, see Install the Industrial Process Manager and Assign Industrial Process Manager user roles.

Industrial Workspace Admin Guided Setup

If you have the admin role, you can use the Guided Setup to lead you through the setup of the Industrial Process Manager application.

To access the Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

The specific steps that appear as unlocked in the Guided Setup depend on which applications you have installed in your instance.

If only the Industrial Process Manager is installed, the following setup functions are locked:

- The Industrial Workspace setup steps.
- The Operational Technology Manager setup steps.
- Any Industrial Process Manager steps that depend on the Operational Technology Manager.
- The Operational Technology Vulnerability Response setup steps.
- The Operational Technology Incident Management setup steps.
- The Operational Technology Change Management setup steps.
- The Operational Technology Knowledge Management setup steps.
- The Operational Technology Request Management setup steps.

To learn more about Guided Setups and their use, see Using guided setup.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign Industrial Process Manager user roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Industrial Process Manager application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following table can use the Industrial Process Manager application.

Role	Description
Equipment Model Viewer [cmdb_ot_isa_viewer]	Can only view the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] table records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models.
Equipment Model Editor [cmdb_ot_isa_editor]	Can view and edit the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models.
Equipment Model Admin [cmdb_ot_isa_admin]	Inherit the cmdb_ot_isa_editor role and can also do the following actions: • Use the Industrial Guided Setup to set up the Industrial Process Manager and the Operational Technology Manager. • Edit the Equipment Model Template [isa_entity_template], [isa_entity_level], and Equipment Entity type [isa_entity_type] table records. To learn more, see Industrial Workspace Admin application menu and Guided Setup.
Equipment Model Downtime Planner [sn_isa_schedule_admin]	Can create, modify, and delete equipment entity schedules. Can also associate schedules with equipment entities.
Equipment Model Viewer All [cmdb_ot_isa_viewer_all]	Can view all ISA Equipment Model records (cmdb_ci_ot_isa_entity) and associated Equipment Model Template records (isa_entity_template, isa_entity_level, isa_entity_type). Role included with cmdb_ot_admin.
Amazing Admin [sn_ot_amazing_admin]	Can create, modify, and delete OT subnet records (ot_subnet_mapping) for all the equipment model entity OT subnet system properties.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role	Description
Amazing Editor [sn_ot_amazing_write]	Can create, modify, and delete OT subnet records (ot_subnet_mapping) for all the equipment model entities associated with the user.
Amazing Viewer [sn_ot_amazing_read]	Can view OT subnet records (ot_subnet_mapping) for all the equipment model entities.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

View and edit OT system properties

View and edit all of the Operational Technology (OT) related system properties for different applications.

Before you begin

Role required: admin or cmdb_ot_isa_admin

About this task

You can modify the system properties for the following OT applications from **All OT Properties** module on the ServiceNow AI Platform.

- IT Discovery for OT Networks
- Industrial Process Manager
- ISA Equipment Model
- Operational Technology Manager
- Operational Technology Incident Management
- Operational Technology Knowledge Management
- Operational Technology Change Management
- Industrial Workspace Common

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **All OT Properties**.
2. In the System Properties table, select the application that you want to edit the system properties for.
3. Edit the available system properties as needed for the application or feature.
4. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Defining equipment model templates

Create templates that you can assign to the equipment model entities that you created in the ServiceNow AI Platform. You can use these templates to characterize an equipment model or structure the data that describes your physical industrial facility by grouping similar types of equipment model entities.

Create an equipment model template

Create an equipment model template record that identifies and describes the use of the template. After you create an equipment model template, you can create hierarchical levels and types for it.

Before you begin
Role required: cmdb_ot_isa_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Template**.
2. Select **New**.
3. On the form, fill in the fields.

Equipment model template form

Field	Description
Name	Name of the equipment model template.
Description	Description of the equipment model template.
Application	Selected application scope. Global appears if this scope is the global application scope.

4. Select **Submit**.

What to do next
Create hierarchical sorting levels for the equipment model template.

Create hierarchical sorting levels for equipment templates

Create and assign hierarchical levels for your equipment model template. When you assign an equipment template to an equipment model, these levels sort and structure the data you see in it.

Before you begin
Role required: admin

About this task
You can assign levels to an equipment model template for sorting purposes. For example, you can assign Site, Area, Work Center and other levels to the equipment, and designate the sorting sequence for each.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Template**.
2. Select an equipment model template.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. In the Template Levels related list, select **New**.
4. On the form, fill in the fields.

Template Level form

Field	Description
Level name	Name of the level to which you are assigning the equipment model. Examples include: **Site** An industrial site. **Area** An area in an industrial site. **Work Center** A work center in an industrial site.
Parent	Identifier for the equipment model template level before this level. If left empty, this level is the top level in the model. For example, you can do the following actions: ○ If you're creating a Site level, leave this field empty if it is the top level of the equipment model hierarchy that does not have a parent. ○ If you're creating an Area level, and it is a child to the Site level, select **Site** as its parent. ○ If you're creating a Work Center level, and it is a child to the Area level, select **Area** as its parent.
Application	Selected application scope. Global appears if this scope is the global application scope.
Template	Name of the selected equipment model template.
Order	Number that indicates the position of the level in the equipment model hierarchy for sorting purposes. The smallest number entered represents the highest hierarchical level. For example, enter `1` for Site if the site represents the highest level in the hierarchy for the equipment model template.

5. Select **Submit**.

What to do next

Create granular types within an equipment model template hierarchical level.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create equipment model level types

Create granular level types within each equipment model template level that you created. The granular level types that you create within that level describe the type of production processes within it.

Before you begin
Role required: admin

About this task
You can create types that represent the different types of locations, areas, or functions within a level. For example, in the ISA 95 template, the Work Center level has the following level types:

- Production Cell
- Production Unit
- Production Zone
- Storage Zone

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Template**.
2. Select an equipment model template.
3. In the Template Levels related list, select an equipment model template level.
4. In the Template Types related list, select **New**.
5. On the form, fill in the fields.

Template Level Type form

Field	Description
Level type name	Name of the level type that you're assigning to the selected equipment model template level. For example, you assign Production Cell to create a Production Cell type for a Work Center level.
Level name	Name of the selected equipment model template level.
Application	Selected application scope. Global appears if this scope is the global application scope.
Template	Name of the selected equipment model template.

6. Select **Submit**.

Importing equipment model data

The scheduled import function enables you to import your existing equipment model data from a populated Microsoft Excel flat-file spreadsheet. You can use it to import your ISA-95 Equipment Model data to the Configuration Management Database (CMDB).

You must install the Industrial Process Manager before importing equipment model data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Several methods are available for importing the equipment model data into the ServiceNow AI Platform:

1. If you use the spreadsheet to import the data, you must populate the Microsoft Excel spreadsheet with your existing ISA-95 Equipment Model data and run the **SG-Equipment Model Scheduled Import Using Spreadsheet** scheduled import. Many legacy record systems contain functions that enable you to export this data to an Excel spreadsheet, which means that you don't have to populate it manually.
2. Several ServiceNow partners are also developing integrations to third-party legacy record systems that store equipment model data.
   - When these integrations are available, you can find them on the ServiceNow Store by searching for Operational Technology certified integrations for the Industrial Process Manager.
   - Install those integrations that are applicable to your environment, and run them as needed.

By using these import methods, you can update existing equipment models in the ServiceNow AI Platform with the data that is stored in your authoritative source when needed. For newly imported data, the ServiceNow AI Platform automatically creates Equipment Model Entity CI class records in the Configuration Management Database (CMDB).

System properties that affect import processing

The following system properties affect how you populate your Microsoft Excel spreadsheet with the equipment model data and how the Import Equipment Model - ETL process functions.

sn_isa_model.cmdb_relationships_sync_levels

Determines how many levels of an equipment model can be imported into the ServiceNow AI Platform and then are synchronized in the Configuration Management Database (CMDB). The default value is 8.

sn_isa_model.short_code_validation_max_length

Sets the maximum length for the Short Code column on your spreadsheet. The default value is 3.

sn_isa_model.user_search_matching_attribute

Matches the user data references that are imported from your populated spreadsheet to the corresponding user records that are stored in the System Users [sys_user} table. The default is the user's email address, because the email address is unique to each user record.

glide.scriptable.excel.max_file_size

Sets the maximum size of an Excel file, expressed in bytes. This property is global.

Note: To learn more about adding or creating system properties to control system behavior, see Add a system property.

Populating your Microsoft Excel spreadsheet with equipment model data

Create and populate a Microsoft Excel spreadsheet with your existing ISA equipment model data. Positioning your existing data in the correct columns is crucial to the success of your upload.

To create a Microsoft Excel spreadsheet that properly populates the Configuration Management Database (CMDB) in the ServiceNow AI Platform, do the following actions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Prepare your spreadsheet for upload by using the Microsoft Excel spreadsheet that is attached to the data source record. To locate an empty template, do the following actions:
   a. Navigate to **Equipment Model - ISA** > **Import Equip. Model - Data Source**
   b. Click **Import Equipment Model – Data Source - v2.xlsx**

   Note: Alternately, to download the **Import Equipment Model – Data Source - v2.xlsx** spreadsheet, see the Microsoft Excel spreadsheets required for the ISA Equipment Model Excel Service Graph Connector [KB0966600] article in the Now Support Knowledge Base.

2. Download the attached Import Equipment Model – Data Source - v2.xlsx spreadsheet to learn more about the template and its worksheets:

   Note: If you're an ISA SGC user upgrading from v1 to v2, see the section named **Upgrading from v1 to v2** below.

   Import Equipment Model – Data Source - v2.xlsx spreadsheet

Worksheet name	Purpose
Blank template for data import	Populates your Equipment Model data for import. You can view detailed examples in the remainder of this topic.
Data Column Descriptions	Provides descriptions of the data columns on the spreadsheet, similar to the information found in this topic.
Sample Data for Import	Provides an example of an equipment model for import in the spreadsheet. You can view these examples in the remainder of this topic.

3. After populating the Microsoft Excel spreadsheet, save it in a known location for easy access when you run the Integration Hub ETL function.

   Note: Column names cannot be changed. You can add additional columns to support additional fields to uniquely identify owners, as designated in the *sn_isa_model.user_search_matching_attribute* system property.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Populating the spreadsheet

Sample Operational Technology data, columns A through J

You can import data from multiple sites in a single spreadsheet. The example image shows data for two sites: ATL and CTL.

	A	B	C	D	E	F	G	H	I	J
1	Path	Short Code	Entity Name	Location	Assigned to	Support Group	Description	Process criticality	Company	Template
2	ATL	ATL	Atlanta Site	Altlanta Car Facility	fred.luddy@example.com	Atlanta Plant Support	the site in Atlanta where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
3	ATL-B64	B64	Building 64	Altlanta Building 64	fred.luddy@example.com	Atlanta Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template
4	ATL-B42	B42	Building 42	Altlanta Building 42	fred.luddy@example.com	Atlanta Plant Support	similar to building 64 except with a 42 on the side	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
5	ATL-B64-MASS	MASS	Model M	Altlanta Building MASS	fred.luddy@example.com	Atlanta Plant Support	model S needs to be assembled somewhere	1 - most critical	Demo Car Corp	ISA 95 Default Template
6	ATL-B64-QASS	QASS	Model Q	Altlanta Building QASS	fred.luddy@example.com	Atlanta Plant Support	a place for the Q model to get assembled	1 - most critical	Demo Car Corp	ISA 95 Default Template
7	ATL-B64-MPROD	MPROD	Model MPROD	Altlanta Building MPROD	fred.luddy@example.com	Atlanta Plant Support	Model S also needs a production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
8	ATL-B64-QPROD	QPROD	Model QPROD	Altlanta Building QPROD	fred.luddy@example.com	Atlanta Plant Support	Model Q production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
9	ATL-B42-MQSTOR	MQSTOR	Model M and Q	Altlanta Building MQSTOR	fred.luddy@example.com	Atlanta Plant Support	storage for the models we built	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
10	ATL-B64-QPROD-C1	C1	Cell 1	Altlanta Building C1	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 1	1 - most critical	Demo Car Corp	ISA 95 Default Template
11	ATL-B64-QPROD-C2	C2	Cell 2	Altlanta Building C2	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 2	1 - most critical	Demo Car Corp	ISA 95 Default Template
12	ATL-B42-MQSTOR-Z1	Z1	Zone 1	Altlanta Building Z1	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ for transfer	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
13	ATL-B42-MQSTOR-Z6	Z6	Zone 2	Altlanta Building Z6	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ to just store the stuff	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
14	CTL	CTL	California Site	California Car Facility	fred.luddy@example.com	California Plant Support	the site in California where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
15	CTL-C64	C64	Building 64	California Building 64	fred.luddy@example.com	California Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template

Columns A through J

Column	Name	Type	Description	Requ
A	Path	string	Concatenation of the short codes of this entity and all its parent entities. For example, `ATL - B42 - MQSTOR - Z1` is the concatenation of these short codes: • ATL short code for the Atlanta site. • B42 short code for Building B42. • MQSTORE short code for Model M and Q. • Z1 short code for the Zone 1 transfer storage zone for Model M and Q.	Yes
B	Short Code	string, alphanumeric only	Short description code for the entity. Refer to the previous Path column description for examples of short codes. The Short Code can be no longer than the maximum length that is designated in the *`sn_isa_model.short_code_validation_max_length`* system property.	No
C	Entity Name	string	Long name of the entity. For example, a city name, a building number, or a model number.	Yes
D	Location	string	Location of the entity. For example, you would list Atlanta Building 64 for each of the equipment models that are located there. The cmn-location value that is stored in the Configuration Management Database (CMDB) in the ServiceNow AI Platform, which uses it as a reference.	No

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Columns A through J (continued)

Column	Name	Type	Description	Requ
E	Assigned to	string	Email address of the assigned person who owns and manages this entity record. **Note:** You can use additional attributes, based on the settings designated in the *sn_isa_model.user_search_matching_attribute* system property.	No
F	Support Group	string	Name of the group that supports the maintenance and management of this entity.	No
G	Description	string	Long description of this equipment model entity and its purpose.	No
H	Process criticality	string	Measure of how critical, or important, the entity is to the industrial process. Examples are as follows: • 1 - most critical. • 2 - somewhat critical.	No
I	Company	string	Name of the company that the entity belongs to. The cmn-location value that is stored in the CMDB in the ServiceNow AI Platform, which uses it as a reference.	No
J	Template	string	The template used to import data. **Note:** After your import your data, you can't set the template.	Yes

Upgrading from v1 to v2

ISA SGC users upgrading from v1 to v2 can import new ISA equipment model entities with unique paths. Use a fix script to update existing entities.

Import your equipment model data using the data source and scheduled import

After you complete your Microsoft Excel spreadsheet with your equipment model data, import it into the ServiceNow AI Platform by using the data source and scheduled import.

Before you begin

Before you perform this process, you must prepare a Microsoft Excel spreadsheet for import. To learn more, see Populating your Microsoft Excel spreadsheet with equipment model data.

Role required: admin or cmdb_inst_admin

About this task

By running this process, you create unique Equipment Model Entity CI class records in the Configuration Management Database (CMDB) for the equipment model records that are included in your spreadsheet.

Procedure

1. Navigate to **All** > **Equipment Model - ISA** > **Import Equip. Model - Data Source**.
2. In the **SG Equipment Model** data source record, attach the Microsoft Excel spreadsheet that you created:

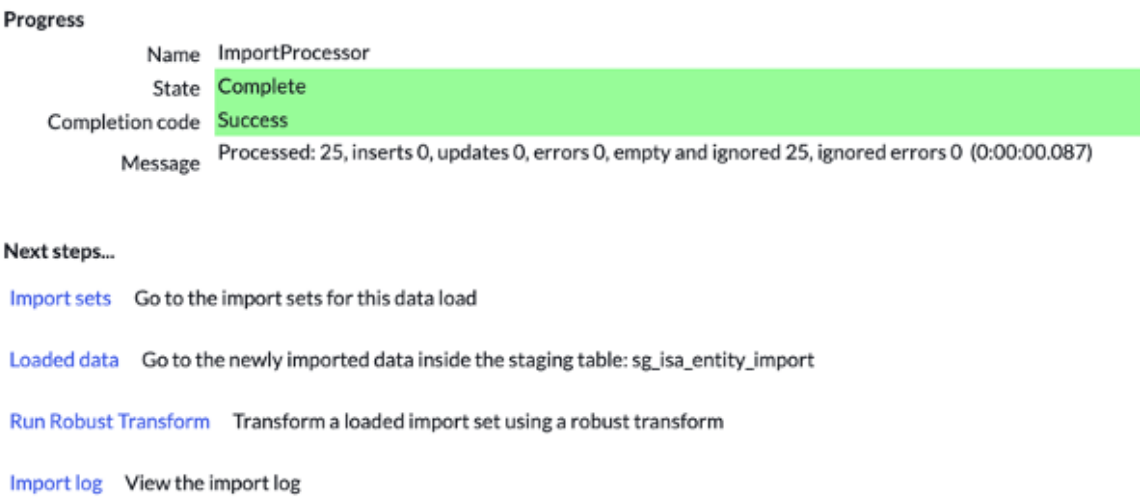
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select **Manage Attachments**.

b. In the Attachments dialog box, select **Choose File**.

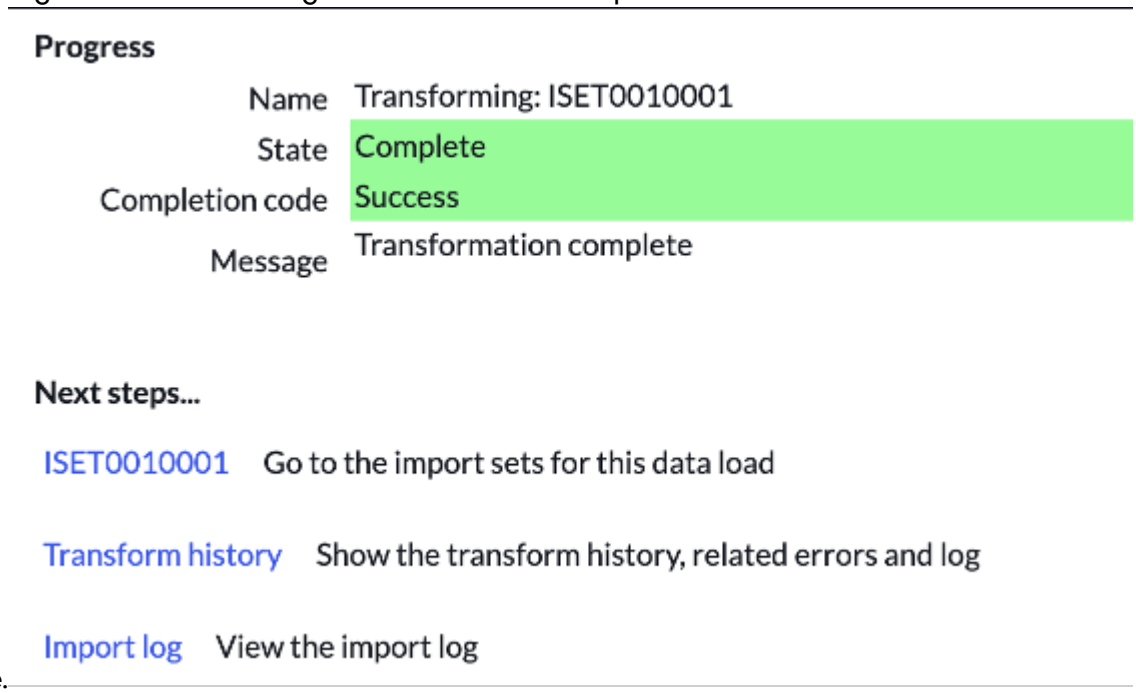
c. Select the Microsoft Excel spreadsheet that you created, and then close the Attachments dialog box.

d. After attaching the spreadsheet, select the **Load All Records** related link to load all records from the spreadsheet to the import table. Once the operation is complete, you should see the following confirmation message with the **Success** completion code if the data is loaded without any errors.



e. In the confirmation message, select the **Run Robust Transform** related link.

f. Select **Transform**. If the import is successful, you should see the following confirmation message with the **Success** completion code.



Manage equipment model site access for non-administrators

Assign or remove non-administrator access to equipment model sites. You can create the user criteria to determine whether certain users can access the equipment model entities for specific sites.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
Use the user criteria to determine whether certain users can read or edit equipment model entities for specific sites. After you create a user criteria record, you can assign it to a site to control who can read and edit the equipment model entities. You can further assign the OT roles to users or groups to enable them access to OT devices that are assigned to those same sites. For more information, see Assign Operational Technology Manager roles.

Note: For those users that are upgrading to version 1.0.12, their site user access is migrated to user criteria and groups. For more information, see Migrating site user access to user criteria and groups.

Procedure
1. Navigate to **All** > **Knowledge** > **Administration** > **User Criteria**
2. Select **New**.
3. On the form, fill in the fields.
   For a description of the field values, see User criteria form.

What to do next
After you create the user criteria, you can assign it to a site. For more information about assigning the Can Edit access to a site, see Assign user criteria for Can Edit access to a site. For more information about adding the Can Read access to a site, see Assign user criteria for Can Read access to a site.

Assign user criteria for Can Read access to a site

Assign the user criteria to a site to define which users can read or view the equipment model entities that belong to the selected site.

Before you begin
Role required: cmdb_ot_isa_admin or admin

About this task
You can assign the user criteria for Can Read access in two locations:

- From the Equipment Model Entity View Access table
- From the Can Read Equipment Models related list in a site record

Procedure
1. Navigate to either the table or related list.

Location	Navigation path
Equipment Model Entity View Access Table	**All** > **Equipment Model - ISA** > **User Criteria - Can Read**
Can Read Equipment Models related list	**All** > **Equipment Model - ISA** > **Sites** and open a site record. Select the Can Read Equipment Models related list.

2. Create a record by selecting **New**.
3. In the **Site** field, select the equipment model site record that you need.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the **User Criteria** field, select the user criteria to define which users can read or view the selected site's equipment model entities.

   Note: If a user has the cmdb_ot_viewer role, the user can also view the Operational Technology (OT) devices that are assigned to the selected site.

   If a user has a cmdb_ot_editor role, the user can edit the OT devices that are assigned to the selected site.

5. Select **Submit**.

Assign user criteria for Can Edit access to a site

Assign the user criteria to a site to define which users can edit the equipment model entities that belong to the selected site.

Before you begin
Role required: cmdb_ot_isa_admin or admin

About this task
You can assign the user criteria for Can Edit access in two locations:

- From the Equipment Model Entity Edit Access table
- From the Can Edit Equipment Models related list in a site record

Procedure

1. Navigate to one of the following locations.

Location	Navigation path
Equipment Model Entity View Access Table	**All** > **Equipment Model - ISA** > **User Criteria - Can Edit**
Can Edit Equipment Models related list	**All** > **Equipment Model - ISA** > **Sites** and open a site record. Select the Can Edit Equipment Models related list.

2. Create a record by selecting **New**.
3. In the **Site** field, select the equipment model site record that you need.
4. In the **User Criteria** field, select the user criteria to define which users can edit the selected site's equipment model entities.

   Note: If a user has the cmdb_ot_viewer role, the user can also view the Operational Technology (OT) devices that are assigned to the selected site.

   If a user has a cmdb_ot_editor role, the user can edit the OT devices that are assigned to the selected site.

5. Select **Submit**.

Equipment Model entity access control tables

Equipment Model entity access control tables store permissions that determine which users or groups can view or modify equipment model entities. By default, users and groups can view (read) equipment model entities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Base and extension tables

The access control tables provide the data model foundation for fine-grained access control over Operational Technology (OT) equipment model entities. These tables enable ISA administrators to assign access permissions based on individual users or user groups.

The access control data model consists of a base table and two extension tables, all within the ISA Equipment Model (`sn_isa_model`) scope:

- Equipment Model Entity Access [`isa_entity_access`]: the base table that stores the entity, the entity site, and whether the grant allows editing.
- Equipment Model Entity User Access [`isa_entity_user_access`]: extends the base table to assign access to individual users.
- Equipment Model Entity Group Access [`isa_entity_group_access`]: extends the base table to assign access to user groups.

The base table contains three key fields: the entity reference, the entity site reference (limited to top-level entities), and a Boolean field that controls whether edit access is permitted. Each extension table adds a specific field to support its access assignment method.

Access scope and granularity

Entity-level access control is more granular than site-level access control. Site-level access controls apply to an entire equipment model entity site, while entity-level access controls apply to individual entities within a site. This granularity enables you to assign different permission levels to different equipment model entities within the same site hierarchy.

Access assignment methods

The two extension tables support different approaches to assigning access.

Access assignments

Access level	Description
User-based access	Assigns permissions to individual user accounts. Use this method when specific users need access to particular entities.
Group-based access	Assigns permissions to user groups. Use this method to grant access to all members of a team or department.

For more information on ISA access levels, see ISA Access by User or ISA Access by Group.

Permission levels

Access records provide two permission levels.

Permission levels

Permissions	Description
Read-only access	Users can view the entity but cannot modify it. This is the default permission level.
Edit access	Users can view and modify the entity. This permission is granted when **Active** is set to true.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Validation rules

The access control tables enforce two key validation rules:

- The entity site field is required. Select a site before you can assign access to an entity.
- The entity field is hidden until you select a site. After you select a site, the entity field displays only entities that belong to that site.

Connection between OT devices and Equipment Model entities

OT devices and Equipment Model entities represent different aspects of your operational technology environment:

- **OT devices**: The actual physical or virtualized devices discovered in your network (controllers, sensors, gateways, and similar equipment).
- **Equipment Model entities**: The logical hierarchy that represents how equipment is organized and relates to production processes. Equipment Model entities follow ISA-95 standards.

The **Mapped ISA Entity** field on OT devices links physical devices to logical entities. This mapping enables access control to apply consistently across both representations of your OT environment.

When you grant a user access to an Equipment Model entity, that user also gains access to OT devices mapped to that entity (subject to site-level permissions).

For more information on the Mapped ISA entity, see Mapped ISA Entity field.

Legacy query business rule

The existing query business rule on the OT Entity [`cmdb_ot_entity`] table is turned off. Row-level access is now handled entirely by the read ACL rules.

Note: This information was developed with assistance from the AI tool, Claude.

ISA Access by User

ISA Access by User lets you assign view or edit permissions to individual users for specific equipment model entities. Use this method when particular users need access to equipment model entities.

How user-based access works

When you assign access to a user, you specify which equipment model entity they can access and what permission level they have: view or edit. View access lets the user see the entity in read-only mode. Edit access lets the user view and modify the entity.

Each user access record is independent. You can grant one user view access to an entity while granting another user edit access to the same entity.

When to use user-based access

Use user-based access when granting permissions to specific individuals. This approach is most effective when:

- A small number of users need access to particular entities
- Users have different permission levels for the same entity
- Access requirements change frequently for individual users

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For larger groups with the same permissions, group-based access is more efficient.

Who manages user-based access

Only users with the `cmdb_ot_isa_admin` role can create, read, update, or delete user-based access records. The ISA Access - By User navigator module provides a dedicated list view for managing user access assignments.

Note: This information was developed with assistance from the AI tool, Claude.

Assign ISA Access edit permissions by user

Configure access permissions to grant users edit access to Equipment Model entities.

Before you begin

Role required: cmdb_ot_isa_admin or admin

About this task

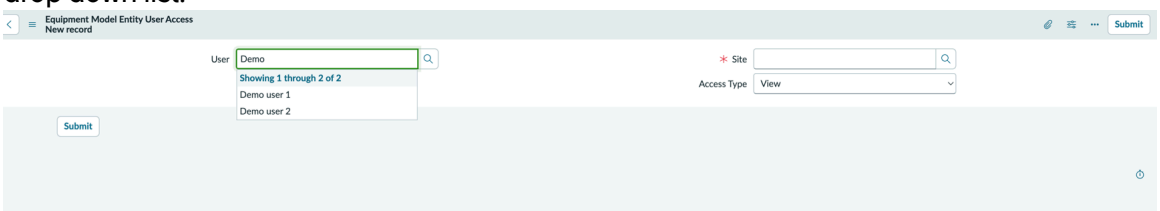
The Equipment Model entity access control interface lets you manage which users or groups can access specific Equipment Model entities and what actions they can perform. By default, users and groups have read-only access.

Procedure

1. Navigate to **All** > **Equipment Model - ISA** > **ISA Access - by User**.
   The Equipment Model Entity User Access page opens, showing a list of users with current access assignments.



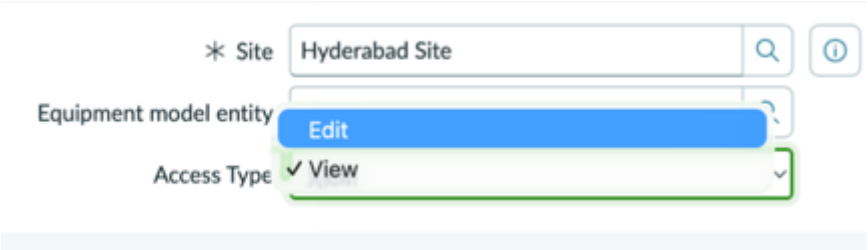
2. On this page, select **New**.
   The new record form opens.
3. In the **User** field, enter a new user name or select the search icon and select a user from the drop down list.



4. In the **Site** field, select the site for this user's access.
   The a Site selection is required.
5. When you select a **Site**, the **Equipment model entity** field is displayed.
6. In the **Equipment model entity** field, select the Search icon.
   The Equipment Model Entities list for the chosen site opens.
7. Select an entity that is available in the Site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. From the **Access Type** field, select **Edit** from the menu.



9. Select **Submit**.
   The new record is added to the Equipment Model Entity User Access list and the user now has edit permissions.
10. To modify access for an existing user, select the user from the Equipment Model Entity Group Access list, update the Access Type setting, and select Update.

Result
The user can now access the Equipment model entity at both the read and edit levels. The user's access is scoped to the selected site and is effective immediately.

ISA Access by Group

ISA Access by Group lets you assign view or edit permissions to user groups for specific equipment model entities. Use this method when all members of a team or department need the same access level to particular entities.

How group-based access works

When you assign access to a group, all members of that group receive the permission level you specify: view or edit. View access lets group members see the entity in read-only mode. Edit access lets group members view and modify the entity.

When you add or remove users from a group, their access to equipment model entities updates automatically based on the group's permissions.

When to use group-based access

Use group-based access when multiple users need the same permissions to particular entities. This approach is most effective when:

- Multiple users in a team or department need identical access
- You want to manage access for large numbers of users efficiently
- User membership in groups changes over time
- You want permissions to apply automatically to new group members

For access requirements unique to individual users, user-based access is more appropriate.

Who manages group-based access

Only users with the `cmdb_ot_isa_admin` role can create, read, update, or delete group-based access records. The ISA Access - By Group navigator module provides a dedicated list view for managing group access assignments.

Note: This information was developed with assistance from the AI tool, Claude.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign ISA Access edit permissions by group

Grant groups edit access to specific equipment model entities for ISA Access.

Before you begin
Role required: cmdb_ot_isa_admin or admin

About this task
The Equipment Model Entity access control interface lets you manage which groups can access specific equipment model entities and what permission level they have. By default, groups have read-only access. Use this procedure to grant edit access to a group for a specific equipment model entity at a site.

Procedure
1. Navigate to **All** > **Equipment Model – ISA** > **ISA Access – By Group**.
   The Equipment Model Entity Group Access page opens, showing groups with current access assignments.
2. Select **New** to create a group access record.
3. In the **Group** field, enter a group name or select the search icon and select a group from the list.
4. In the **Site** field, select the search icon to select a site related to this group.
   A site selection is required.
5. In the **Equipment Model Entity** field, select the search icon and select an entity available from this site.
6. From the **Access Type** list, select **Edit**.
7. Select **Submit**.
   The group access record is added to the Equipment Model Entity Group Access list.

Result
The group can access the equipment model entities with edit permissions. The access is scoped to the selected site and takes effect immediately.

Mapped ISA Entity field

The Mapped ISA Entity reference field for mapped OT devices identifies which Equipment Model entity the device is automated by. The mapped ISA entity is associated to a site.

Field definition

Mapped ISA Entity field properties

Property	Value
Field name (API)	*mapped_isa_entity*
Field label	Mapped ISA Entity
Field type	Reference field
References table	[*cmdb_ci_ot_isa_entity*]
Location	Industrial workspace OT device lists only
Visibility on forms	Not visible on any form (platform or workspace)
Default edit mode	Read-only for most users

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field behavior

The Mapped ISA Entity field displays only ISA entities related to the OT device through Automates relationships in the same site. When a device has no mapped ISA entity, the field is empty in workspace lists.

Field access control

Mapped ISA Entity field ACL rules

Access level	Roles required	Additional condition
Read	cmdb_ot_viewer and cmdb_ot_isa_viewer	None
Write	cmdb_ot_editor and cmdb_ot_isa_viewer	User must have full site-level access to the device site
Report view	cmdb_ot_isa_viewer	Admins cannot override

Workspace list visibility

The Mapped ISA Entity field appears in the following Industrial workspace OT device lists:

- All OT Devices list
- OT Control System list
- OT Field Devices list
- OT Network Devices list
- Unclassed OT Devices list

In each list, the field appears immediately after the *isa_entity_site* column.

The field does not appear in platform list views of the OT devices table.

Note: This information was developed with assistance from the AI tool, Claude.

Edit the Mapped ISA Entity on an OT device

The Mapped ISA Entity field identifies which ISA entity automates an OT device. Edit this field in Industrial workspace lists to establish the relationship between devices and their controlling entities.

Before you begin

Role required: `cmdb_ot_editor` and `cmdb_ot_isa_viewer`

You must have full site-level access to the OT device's site to edit this field.

About this task

Mapping OT devices to ISA entities establishes the relationship between physical devices and the entities that control them. This mapping enables better asset tracking and operational visibility.

Edit the Mapped ISA Entity field in Industrial workspace OT device lists. This field is read-only in platform views and on forms. The reference picker displays only ISA entities related to the OT device via Automates relationships within the same site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to Industrial Workspace.
2. Open an OT device list view.

   Available workspace lists:

   - All OT Devices
   - OT Control System
   - OT Field Devices
   - OT Network Devices
   - Unclassed OT Devices
3. In the Mapped ISA Entity column, select the field for the OT device you want to edit.

   The Mapped ISA Entity column appears after the Site column. The reference picker displays only ISA entities related to this device via Automates relationships in the same site.
4. Select an ISA entity from the picker.

   If no entities appear, verify that ISA entities are related to this OT device via Automates relationships in the same site. To clear the field, select the empty option.
5. Press **Enter** or select outside the field to save the change.

Result

The OT device record now displays the selected ISA entity in the Mapped ISA Entity field. Users with access to that ISA entity can view this mapping in workspace lists.

Note: This information was developed with assistance from the AI tool, Claude.

Managing an equipment model entity schedule

You can manage an equipment model entity schedule with the Industrial Process Manager application. By using a schedule, you can track several maintenance tasks for one equipment model entity.

Equipment model entity schedule overview

You can link schedules to any equipment model entity. If you have the Equipment Model Downtime Planner role (sn_isa_schedule_admin), you can add, modify, or delete the schedule entries of an equipment model entity and do the following tasks:

- Maintain the schedules for the various equipment model entities.
- Associate these schedules with equipment model entities.
- Pick a time slot from a schedule so that you can work on an Operational Technology (OT) incident or remediation task. For more information, see Select a start time for an OT remediation task.

Examples

Let's say that you want to set multiple schedule entries for one equipment model entity schedule. These entries complete different tasks and occur at different times. You can do so by creating schedule entries in the Schedule Entries related link of the existing equipment model entity schedule record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you no longer want a schedule associated with an equipment model entity, you can detach it. Use the Schedules related link in the equipment model record.

To view existing schedules for an equipment model entity, use the Equipment Model Manager or the Planned Downtime module. Both options are available on the Platform.

Create an equipment model entity schedule

Create an equipment model entity schedule with the Industrial Process Manager application. With these schedules, you can easily maintain multiple equipment model entities.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Entity Schedules**.
2. Select **New**.
3. On the form, fill in the fields.

Equipment model entity schedules form

Field	Description
Name	Unique name for the schedule.
Time zone	Time zone for the schedule. If you select **Floating**, the time zone is relative to whatever process is accessing the item at. Floating schedules don't change across time zones. All users see 8:00-17:00 as 8:00-17:00 regardless of location.
Type	Text label that describes the purpose of the schedule.
Description	Description of the schedule.

4. Select **Submit**.

What to do next

Now, you can create the entries for an equipment model entity schedule. For more information, see Create a schedule entry.

Create a schedule entry

Create a schedule entry for an existing equipment model entity schedule in the Industrial Process Manager application. You can create more than one entry for a schedule. Schedule entries include multiple maintenance tasks for one equipment model entity.

Before you begin

Role required: sn_isa_schedule_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Entity Schedules**.
2. Select an existing equipment model entity schedule record.
3. Select the **Schedule Entries** tab.
4. Select **New**.
5. On the form, fill in the fields.

Schedule entries form

Field	Description
Name	Unique name for the schedule entry.
Type	Label that describes the purpose of the schedule.
Show as	Option that indicates how the schedule entry should appear in calendar applications.
Repeats	Repetition interval for the schedule entry, if any. If you select a repetition interval, other fields appear so that you can further specify the repeat interval.
Repeat every	Scheduling repetition frequency - weekly, monthly, or yearly. This field appears only when **Daily**, **Weekly**, **Monthly**, or **Yearly** is selected from the **Repeats** field.
Repeat on	Days of the week that a weekly schedule repeats on. This field appears only when **Weekly** is selected from the **Repeats** field.
Monthly type	Monthly schedule repetition frequency. This field appears only when **Monthly** is selected from the **Repeats** field. Options include: ○ Repeat on a specific day of the month. ○ Repeat on a specific day in a specific week of the month. ○ Repeat on the last day of the month. ○ Repeat on a specific weekday in the last week of the month.
Yearly type	Yearly schedule repetition frequency. This field appears only when **Yearly** is selected from the **Repeats** field. Options include: ○ Repeat on a specific day of the year. ○ Repeat on a floating day.
Float week	Week of the month that a floating yearly schedule repeats on. This field appears only when **Floating** is selected from the **Yearly** field.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Float day	Day of the week that a floating yearly schedule repeats on. This field appears only when **Floating** is selected from the **Yearly** field.
Month	Month of the year that a floating yearly schedule repeats on. This field appears only when **Floating** is selected from the **Yearly** field.
Repeat until	Repetition end date. If you leave this field empty, the schedule repeats indefinitely.

6. Select **Submit**.

Result
Your schedule entry is created, and now you can edit and update the entry as necessary.

Associate a schedule with an equipment model entity

Create one or more maintenance schedules for an equipment model entity, edit an existing schedule, or delete schedules with the Industrial Process Manager application.

Before you begin
Role required: sn_isa_schedule_admin

Procedure
1. Navigate to **All** > **Equipment Model - ISA** > **Equipment Model Entities**.
2. Select the equipment model entity that you want to associate with a schedule.
3. Select the **Schedules** tab.
4. **Optional:** To add a new schedule for the selected equipment model entity, do these actions:
   - Select **New**.
   - Fill in the form and select **Submit**.
5. **Optional:** To delete a schedule for the selected equipment model entity, do these actions:
   - Select the schedule that you want to delete.
   - Select **Delete**.
6. **Optional:** To edit a schedule for the selected equipment model entity, do these actions:
   - Select the schedule that you want to edit.
   - Add your changes and select **Update**.

Result
The maintenance schedule is created, deleted, or edited. Depending on the steps you followed, an eligible user can see the new schedule, no longer see the deleted schedule, or see the edited version of the schedule.

Attach a schedule to an equipment model entity

Attach an existing schedule to an equipment model entity with the Industrial Process Manager application. Attaching a schedule to an equipment model entity applies the schedule and its entries to that entity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_isa_schedule_admin

Procedure
1. Navigate to **All** > **Equipment Model - ISA** > **Equipment Model Entities**.
2. Select an equipment model entity record.
3. Select the **Schedules** tab.
4. Select **Edit**.
5. In the Collection list, select the schedule that you want to attach to the equipment model entity.
6. Move the selected schedule to the Schedules list by using the middle arrows.
7. Select **Save**.

Result
The attached schedule is now applied to the equipment model entity. You can view and manage the attached schedule in the equipment model entity record.

Detach a schedule from an equipment model entity

Detach an existing schedule from an equipment model entity with the Industrial Process Manager application. If a schedule no longer applies to an equipment model entity, you can easily remove it so that it doesn't show up for that entity.

Before you begin
Role required: sn_isa_schedule_admin

Procedure
1. Navigate to **All** > **Equipment Model - ISA** > **Equipment Model Entities**.
2. Select an equipment model entity record.
3. Select the **Schedules** tab.
4. Select **Edit**.
5. In the Schedules List, select the schedule that you want to detach from the equipment model entity.
6. Move the selected schedule to the Collection list by using the middle arrows.
7. Select **Save**.

View a schedule for the equipment model entity

View a schedule for an existing equipment model entity in the Industrial Process Manager application.

Before you begin
Role required: cmdb_ot_isa_viewer

About this task
You can view equipment model entity schedules in two places depending on where you're working:

- The Equipment Model Manager
- The Planned Downtime module on the Platform

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To view the equipment model entity schedules in the Equipment Model Manager, do these actions:
   a. Navigate to the **Equipment Model Manager**.
   b. Select an equipment model entity record.
   c. Select **View schedules**.
   d. View the downtime slots for that equipment model entity.
2. To view the equipment model entity schedules in the Planned Downtime module, do these actions:
   a. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Planned Downtime**.
   b. View the association of the schedules and equipment model entities.

Add a child schedule

Add a child schedule to an existing equipment model entity schedule with the Industrial Process Manager application. When you make adjustments to the child schedule, it also applies to the parent schedule. For example, you might want to extend the scheduled time on a particular day or remove the holidays from a schedule.

Before you begin

Role required: sn_isa_schedule_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Entity Schedules**.
2. Select a record for an existing equipment model entity schedule.
3. Select the **Child Schedules** tab.
4. Select **Edit**.
5. Select the desired schedule in the Collection list.
6. Move the selected schedule to the Child Schedules list by using the middle arrows.
7. Select **Save**.

Result

The selected child schedule now applies to the parent schedule.

Using Industrial Process Manager with the Operational Technology Manager

After you complete all required set up tasks, including importing equipment models, you can use the Operational Technology Manager and Industrial Process Manager functions on the Industrial Workspace Admin menu. These functions include the Equipment Model Manager and the Industrial Workspace.

The following graphic shows some common questions that industrial personnel ask about operational problems in an enterprise, and the ServiceNow AI Platform functions you use to answer them. These functions help your personnel visualize data relationships in your industrial facilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Industrial personnel questions about operational problems



Betty, a Configuration Manager, works at the enterprise level and wants to know where the OT devices reside in the enterprise. To answer this question, a Configuration Manager can use the Operational Technology Manager functions on the Industrial Workspace Admin menu. To learn more, see Industrial Workspace Admin application menu and Guided Setup.

Bhuvnesh, an OT engineer, works at the site level and wants to know how OT devices map to specific productions processes. For example, a question asked might be "What HMIs and PLCs are controlling this specific portion of the industrial processing? To answer this question, an OT Manager at the site level can use the Industrial Process Manager functions on the Industrial Workspace Admin menu.

Managing equipment models

The Equipment Model Manager in the Industrial Workspace enables you to review and manage ISA-95 equipment model data. You use it to review imported equipment model data or to manually create an equipment model.

Equipment Model Manager in the Industrial Workspace

An equipment model maps the operational elements of a particular facility. For example, an industrial facility in Atlanta that stores materials, and uses them to produce cars. With the Equipment Model Manager, you can view selected equipment model entities and any related records for specific industrial sites. The Equipment Model Manager contains the following functionalities to help you manage the equipment model entities in your OT environment:

- Viewing a graphical representation of an equipment model hierarchy and its relationship to other equipment model entities.
- Viewing or mapping upstream or downstream production processes.
- Reviewing child equipment model entities.
- Reviewing or associating additional OT devices with the selected equipment model entity.
- Adding child equipment model entities to your favorites and updating your view to show only your favorites.
- Keeping record context available when viewing or creating multiple records by opening the records in a single row of tabs.

Note: Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Review and update the equipment model details

Review and update the details for an equipment model that you imported into the ServiceNow AI Platform so that you can make sure that the information is correct. You can also manually create a new equipment model entity and then add details to it.

Before you begin

Import equipment model data to the ServiceNow AI Platform. To learn more, see Importing equipment model data.

Role required: cmdb_ot_isa_viewer, cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

If you have an assigned cmdb_ot_isa_viewer role, you can only view equipment model entities. If you have any of the other assigned cmdb_ot_isa roles, you can also edit equipment model entities.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
   You can search for a site by typing in the site name or its short code.
3. Review an existing equipment model entity, or create one.

Task	Description
Review and update an existing equipment model	In the selector pane, do the following actions: **a.** Expand the equipment model hierarchy. **b.** Click the entity that you want to view.
Create an equipment model entity and populate the details	**a.** Click **Create new entity**. **b.** In the Create new entity form, fill in the details. To learn more, see Create an entity for a new equipment model. **c.** Click **Save**. **d.** Use the Equipment model view details form to enter the remaining details for the new equipment model entity.

4. On the form, review and update the fields.

Equipment model details form

Field	Description
Entity name	Name of the equipment model entity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: You can update the Entity name field after the equipment model entity is created. Updating this field also updates the tree component and site filter. For more information, see Update the entity name or parent of an equipment model entity.
Parent	Name of the entity, if any, that is the parent to this equipment model entity. This field is empty for the top-level parent entity, which has no parent. The top-level parent entity is referred to as a site. **Note:** You can update the Parent field after the equipment model entity is created. Updating this field also updates the tree component and site filter. For more information, see Update the entity name or parent of an equipment model entity.
Template	Equipment model template that is assigned to an equipment model entity you manually create. **Note:** You can't assign an equipment model template to an equipment model that you imported into the ServiceNow AI Platform® using the Integration Hub ETL or a third-party integration.
Level	Hierarchical level that is assigned from the selected equipment model template for data sorting and structuring purposes. Examples are as follows: **Site** Industrial site. **Area** Area in an industrial site. **Work Center** Work center in an industrial site. Search for and select an equipment level to assign to the equipment model entity. To learn more, see Create hierarchical sorting levels for equipment templates.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Type	Name of the level type that is assigned to the equipment model template level. For example, Material Assembly or Production Cell for a Work Center level. To learn more, see Create equipment model level types.
Short description	Short description of this equipment model entity and its purpose.
Short Code	Short code that is assigned to this equipment model entity.
Path	Concatenation of the short codes of this equipment model entity and all its parent entities. For example, `ATL - B42 - MQSTOR - Z1` is the concatenation of the following short codes: ○ ATL short code for the Atlanta site. ○ B42 short code for Building B42. ○ MQSTORE short code for Model M and Q. ○ Z1 short code for the Zone 1 transfer storage zone for Model M and Q.
Location	Location of the equipment model entity. For example, Atlanta Building 64 would be the location for each associated equipment model that is located there. Search for and select the location to assign to the equipment model entity.
Timezone	select the timezone that corresponds to the factory's physical location.
Company	Name of the company that is associated with the equipment model entity. Search for and select a company to assign to the entity.
Assigned to	Assigned user who operates and handles this equipment model entity. Search for and select the user to assign to the entity.
Managed by	Name of the assigned person who owns and is responsible for managing this entity record. Search for and select the user to assign to the equipment model entity.
Process criticality	Measure of how critical, or important, the equipment model entity is to the industrial process. Select the process criticality for the entity. For example: ○ 1 - most critical. ○ 2 - somewhat critical.
Support Group	Name of the group that supports this equipment model entity. Search for and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	select the user group to assign to the equipment model entity.
Managed by Group	Name of the assigned group that owns and is responsible for managing this entity record. Search for and select the user group to assign to the entity.
Company	Name of the company that the equipment model entity belongs to. The core_company value is stored in the CMDB in the ServiceNow AI Platform as a reference.
Operational status	Current operational status of the equipment model entity: **Operational** Entity that is fully operational in the production process. **Non-Operational** Entity that is non-operational in the production process. **Not in use** Entity that is operational but intentionally offline. You can use this value to designate which sites are included for licensing purposes. The sites marked as **Not in use** won't be visible in the Equipment Model Manager of the Industrial Workspace.

5. Review the associated equipment model data in the related list tabs as follows:

Task	Description
View the equipment model hierarchy	See View the equipment model hierarchy.
Map the upstream production processes for the equipment model entity.	a. Click **Upstream Process**. b. To learn more, see Map the upstream production processes for the selected equipment model entity.
Map the downstream production processes for the equipment model entity.	a. Click **Downstream Process**. b. To learn more, see Map the downstream production processes for the selected equipment model entity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
View the child entities for the equipment model entity.	**a.** Click **Child Entities**. **b.** To learn more, see Review the child entities for the equipment model entity.
View the OT devices that are associated with the current equipment model entity and its child entities.	**a.** Click **Mapped OT Devices**. **b.** To learn more, see Add OT devices that are associated with the selected equipment model entity. **Note:** By default, you cannot see OT control modules in this list.

6. When you finish reviewing and updating the equipment model details, do one of the following actions.

Action	Description
Save the updated equipment model entity	Click **Save**.
Delete the equipment model entity	Click **Delete**.

What to do next

To view the roll up for OT data associated with the equipment model entity and its child entities, you can use the following related lists in the equipment model entity record. The roll up view represents the OT devices, OT incidents, OT changes, and so on that automate the entire hierarchy of an equipment model entity.

- Mapped OT Devices
- OT Incidents
- OT Change Requests
- Vulnerable Items
- Remediation Tasks

Create an entity for a new equipment model

Create an entity for a new equipment model. You do this task when you want to manually create a new equipment model entity directly in the ServiceNow AI Platform rather than import the equipment model data from an external source.

Before you begin

Role required: cmdb_ot_isa_editor or cmdb_ot_isa_admin

About this task

Users with an cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can access only those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment model view for** field, select a site.
   Search for a site by entering the site name or short code.
3. Select **Create new entity**.
4. In the **Create new entity** window, search for and select the parent entity.

   Note: Search by short code or name.

5. Complete the fields on the form.

Create new entity form

Field	Description
Parent	Name of the entity, if any, that is the parent to this entity. The currently selected equipment model appears as the parent entity. To change the parent, search for and select a different entity that is a parent to the entity that you're creating.
Entity name	Name of the equipment model entity.
Short Code	Short code assigned to this entity.
Entity type	Name of the level type that is assigned to the equipment model template level. For example, Material Assembly or Production Cell for a Work Center level. Search for and select an entity type. For more information, see Create equipment model level types.

6. Select **Save**.
7. In the Details form, complete the additional fields for the equipment model entity.
   For more information, see Review and update the equipment model details.

View the equipment model hierarchy

View a graphical representation of the hierarchical structure of the selected equipment model entity, and its relationships to other entities in the production process.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site you want to view equipment model information for.
   You can search for a site by typing in the site name or its short code.
3. In the selector pane, select the equipment model entity you want to view a graphical representation of its hierarchy and relationship to other entities.
   For example, select the top-level site entity to view a representation of the entire site.
4. To view the hierarchical structure for the equipment model entity, select **View hierarchy**.

Result

The following graphical representation appears for the selected equipment model entity. The currently selected equipment model appears as the parent entity in the hierarchy.

View the equipment model OT device map

View the graphical representation of the selected equipment model entity and its relationship to other Operational Technology (OT) devices in the production process.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment mode view for** field, select the site that you want to view equipment model information for.
   You can search for a site by typing in the site name or its short code.
3. In the selector pane, select the equipment model entity you want to view a graphical representation of its relationship to other devices.
   For example, select the top-level site entity to view a representation of the entire site.
4. To view the equipment model entity's relationships with devices, select **View OT Device Map**.

View the equipment model OT dependency map

View the graphical representation of the hierarchical structure of the selected equipment model entity and its relationship with other entities and devices in the production process.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment mode view for** field, select the site that you want to view equipment model information for.
   You can search for a site by typing in the site name or its short code.
3. In the selector pane, select the equipment model entity you want to view a graphical representation of its hierarchy and relationship to other devices and entities.
   For example, select the top-level site entity to view a representation of the entire site.
4. To view the equipment model entity's hierarchical structure of relationships with other devices and entities, select **View OT Dependency map**.

Map the upstream production processes for the selected equipment model entity

Use the upstream process to review upstream production processes for the selected equipment model entity. You can also create and map a new upstream production process for the equipment model entity.

Before you begin
Role required: cmdb_ot_isa_editor, cmdb_ot_isa_viewer, cmdb_ot_isa_admin

About this task
Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view equipment model information for.
   You can search for a site by typing in the site name or its short code.
3. In the selector pane, expand the equipment model hierarchy and then click the entity that you want to view.
4. To view the upstream production processes for the equipment model entity, click **Upstream Process**.
5. Review the upstream production processes for the equipment model, or map a new one.

Task	Description
Review the upstream production processes for the selected equipment model entity	Proceed to the next step and review the Up stream process form.
Map an upstream production process	**a.** Click **Add**. **b.** In the Map Upstream Process form, enter the name of the new production process en tity that you are creating. **c.** Click **Save**.
Remove an upstream process	Use the Dependency Map view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
	a. Click **View Process**. **b.** Right-click the relationship that you want to delete. **c.** Click **Delete Relationship**. Use the upstream process record. **a.** Select the checkbox next to the upstream process you want to remove. **b.** Select **Delete**. **c.** In the confirmation message, select **Con firm**.

6. Click **Submit**.

Map the downstream production processes for the selected equipment model entity

Use the downstream process to review the downstream production processes for the selected equipment model entity. You can also create and map a new downstream production process for the equipment model entity.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_viewer, cmdb_ot_isa_admin

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with an assigned cmdb_ot_isa_editor role can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
   You can search for a site by typing in the site name or its short code.
3. In the selector pane, expand the equipment model hierarchy and then click the entity that you want to view.
4. To view the downstream production processes for the equipment model entity, click **Downstream Process**.
5. Review the downstream production processes for the equipment model, or map a new one.

Task	Description
Review the downstream production processes for the selected equipment mod el entity	Proceed to the next step and review the Downstream process form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
Map a downstream production process	**a.** Click **Add**. **b.** In the Map Downstream Process form, en ter the name of the new production process entity that you are creating. **c.** Click **Save**.
Remove a downstream process	Use the Dependency Map view. **a.** Click **View Process**. **b.** Right-click the relationship that you want to delete. **c.** Click **Delete Relationship**. Use the downstream process record. **a.** Select the checkbox next to the down stream process you want to remove. **b.** Select **Delete**. **c.** In the confirmation message, select **Con firm**.

6. Click **Submit**.

Review the child entities for the equipment model entity

Review the child entities that are associated with the selected equipment model entity. You can review the relationships of the associated entities that are subordinate to a higher-level entity.

Before you begin

Role required: cmdb_ot_isa_editor, cmdb_ot_isa_admin.

About this task

You can view equipment model entities for any site, if the cmdb_ot_isa_admin role is assigned to you. However, you can only access those sites that an administrator has granted access to, if the cmdb_ot_isa_editor role is assigned to you. To learn more about granting site access, see Manage equipment model site access for non-administrators.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
2. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
   You can search for a site by entering in the site name or its short code.
3. In the selector pane, expand the equipment model hierarchy, and then select the entity that you want to view.
4. To create a child entity, select the **Create new entity** button and fill in the details in the Create new entity form.
   To learn more, see Create an entity for a new equipment model.
5. To view the child entities for the equipment model entity, select **Child Entities**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Additionally, in the **Related Lists** section you can assign a value in the **Processing Order** field to prioritize a child entity for a given site.

   Note: The **Processing Order** value enables you to sort and prioritize a child entity according to its importance and functionality:

   - In an equipment model hierarchy, a lower Processing Order value is prioritized. If the value assigned to one or more child entities are the same, the child entities are sorted alphabetically.
   - In the Equipment Model menu of the Industrial Workspace, the hierarchy of an equipment model entity is based on the Processing Order value assigned to the child entities.
   - In the OT Risk Management tab, all equipment model entities are in sequence according to the Processing Order value assigned to the child entities.

Add OT devices that are associated with the selected equipment model entity

Use OT devices to review the OT devices that are associated with the selected equipment model entity and its child entities. You can also select and associate other OT devices to the selected equipment model entity.

Before you begin

To associate additional OT devices to the selected equipment model entity, both the Operational Technology Manager and Industrial Process Manager applications must be installed.

Role required: To add OT devices, the logged in user has to have a combination of the following assigned roles:

- cmdb_ot_viewer, cmdb_ot_editor or cmdb_ot_admin role
- cmdb_ot_isa_editor or cmdb_ot_isa_admin role

Note: To learn more about assigning user roles, see Assign Industrial Process Manager user roles.

About this task

Users with an assigned cmdb_ot_isa_admin role can view equipment model entities for any site. However, users with assigned cmdb_ot_isa_editor or cmdb_ot_isa_viewer roles can only access those sites that an administrator has granted access to for specific users. To learn more about granting site access, see Manage equipment model site access for non-administrators.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
   You can search for a site by typing in the site name or its short code.
2. In the **Equipment model view for** field, select the site you want to view equipment model information for.
3. In the selector pane, expand the equipment model hierarchy, and then select the entity that you want to view.
4. To view the associated OT devices for the equipment model entity and its child entities, select **Mapped OT Devices**.
5. Review the associated OT devices or the associate additional OT devices to the selected equipment model entity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Description
Review the associated OT devices for the selected equipment model entity	Proceed to the next step and review the OT devices form.
Associate the additional OT devices to the selected equipment model entity	**a.** Select **Add**. **b.** In the OT devices form, select the addition al OT devices that you want to associate with the equipment model entity. **c.** Select **Add** to add them to the OT devices form. **d.** To edit the columns on the table, select the List Actions ( ) icon. Select **Edit columns** to choose the columns you want to display. For example, if you want to display the IP ad dress column for the OT devices, select **IP Address** from the Available columns and select **OK**.
Remove the OT devices from the selected equipment model entity	**a.** In the Mapped OT Devices list view, select the OT devices that you want to remove. **b.** Select **Remove**.

6. Select **Save**.

Update the entity name or parent of an equipment model entity

Update the entity name or parent fields in an equipment model entity record as needed to help keep your equipment model information up to date.

Before you begin

Role required: cmdb_ot_isa_editor

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the equipment model ( ) button.
   Alternatively, you can navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
3. Select the equipment model entity record that you want to update.
4. Update the **Entity name** field or the **Parent** field as needed.
5. Select **Save**.

Result

When you update the **Entity name** or **Parent** fields, the fields are also updated in the tree component in the Equipment Model Manager and the site filter on the Operational Technology (OT) landing page in the Industrial Workspace.

Bulk edit a site's Operational Technology Vulnerability Response assignment group

Use the bulk edit feature to update the Operational Technology Vulnerability Response (OT VR) assignment group field in multiple site records at once.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: cmdb_ot_isa_admin

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. Open the list ( ) view.
3. Under the **Industrial Process Manager** module, select the Sites list.
4. Select the check box next to each OT site that you want to edit.
5. Select the **Edit** button.
6. In the **OT VR assignment group field**, add the Operational Technology Vulnerability Response assignment group for the selected sites.
7. Select **Update**.

Result
The **OT VR assignment group** field is updated for each selected site.

Generate a location hierarchy

When no locations exist, generate a complete location hierarchy for an ISA equipment model entity tree to establish location references that match the ISA hierarchy.

Before you begin
Ensure the sn_isa_model.isa_entity.validate_and_generate_locations system property is enabled. For more information, see ISA Equipment Model system properties.

Role required: cmdb_ot_isa_editor

Procedure
1. Navigate to the Industrial Workspace.
2. Select the Equipment model icon to open the Equipment Model Manager.
3. Select the equipment model entity that needs a location hierarchy.
   If no location records exist in the selected equipment model hierarchy, the following message appears and you can continue with the auto-generation process:

   "Click Auto generate locations to create and synchronize locations with the Equipment Model Entities."

4. To continue, select the **Auto Generate Locations** UI action.

   Note: You can only continue the auto-generation process if no location reference is found for a node. If a location reference is found, the following message appears and you can't continue the auto-generation process:

   "Cannot auto-generate locations because the entity has existing location references."

5. **Optional:** If you have existing location references and want to continue the auto-generation process, delete the references or manually populate them for each equipment model entity.
   a. After deleting or manually populating the location references, verify they're correctly synced in the **Location Validation Map** tab of the equipment model entity record.
   b. Starting at the bottom level of the map, remediate the nodes with the following messages:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- "Invalid Location" - The entity's location parent doesn't match the equipment model entity's parent location.
- "Missing Location" - The entity doesn't have a location assigned to the **Location reference** field.

Once the bottom level has a valid location reference, the messages disappear.

c. Continue this process with each level until all invalid and missing locations are resolved.

d. Continue the auto-generation process by selecting the **Auto Generate Locations** UI action.

Result
A Location [cmn_location] record is created for the equipment model entity and its child entities. The created cmn_location populates **Location** field for the equipment model entity.

What to do next
You can also navigate to the **Location Validation Map** tab in the equipment model entity record to see the populated fields and view the location hierarchy node map.

Search for an equipment model entity

Search for an equipment model entity in the Industrial Workspace so that you can find the entity more quickly and efficiently.

Before you begin
Role required: cmdb_ot_isa_editor

Procedure

1. Navigate to **All** > **Industrial Workspace**.

2. Select the Equipment Model Manager ( ) icon.

3. In the **Search** bar, search for the equipment model entity that you want to view.

Result
The list automatically expands to show the searched equipment model entity. When you have the **Show Favorites** toggle switched on, the list still expands to show the searched equipment model entity.

View all OT devices by managed network

View your Operational Technology (OT) devices by managed network on the ServiceNow AI Platform.

Before you begin
Role required: cmdb_ot_isa_viewer and cmdb_ot_viewer

About this task
The All OT Devices by Managed Network list on the ServiceNow AI Platform is a database view with data populated from the following tables.

- OT Entity [cmdb_ot_entity]
- Configuration Items [cmdb_ci]
- Configuration Item Relationships [cmdb_rel_ci]
- Allocated IP Address [cmdb_ci_allocated_ip_address]
- IP Network Subnet [cmdb_ci_ip_network_subnet]
- Managed Network [cmdb_ci_managed_network]

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the All OT Devices by Managed Network list can help you understand the relationship between OT devices and their network.

For more information about the OT Device Network Connection data model, see the **OT Device Network Connection data model** section of Operational Technology (OT) extension classes.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager**.
2. Select **All OT Devices by Managed Network**.
3. In the list, you can view the following information.

All OT Devices by Managed Network fields

Field	Description
Managed Network	Name of the managed network that the OT device belongs to.
IP Network Subnet Name	Identifier for the specific IP subnet that the OT device belongs to.
Device IP Address	IP address assigned to the OT device that is used for communication and device management.
OT Device	Name of the OT device.
Parent Managed Network	Higher-level managed network that contains or oversees the current managed network.

Filter equipment model entities by operational status

Filter how equipment model entities appear in the Equipment Model Manager on the Industrial Workspace using a system property. Filtering equipment model entities can help you organize the data shown on the Industrial Workspace.

Before you begin

Role required: cmdb_ot_isa_viewer and cmdb_ot_isa_admin

Procedure

1. Navigate to **All** > **Equipment Model - ISA** > **System Properties**.
2. Under **List of equipment model operational statuses that need to be filtered out from the equipment model page**, list the equipment model entities by**Operational Status** that you want removed from view in the Industrial Workspace.

   You can choose from the following options.

   - Operational = 1
   - Non-Operational = 2
   - Repair in Progress = 3
   - DR Standby = 4
   - Ready = 5
   - Retired = 6
   - Pipeline = 7

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Catalog = 8
- Not in Use = 9

For example, if you want to remove equipment model entities with **Operational Status** field values of **Retired** and**Not in Use**, list 6 , 9.

Favorite a child equipment model entity

Favorite a child equipment model entity in the Equipment Model Manager of the Industrial Workspace so that you can access a tailored view of your favorites while working.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the Equipment Model Manager ( ) icon.
3. Next to the child equipment model entity or entities that you want to favorite, select the **Mark as Favorite** ( ) icon.

   Note: You cannot select an ISA site as a favorite.

   If you select a higher level entity as a favorite, the related child entities underneath won't be shown. But if you select a lower level child entity, the full hierarchy including the parent entity is shown.

4. **Optional:** To remove a child entity from your favorites, select the **Remove as Favorite** ( ) icon.

Result

The child equipment model entities are added to your favorites as per your needs.

To view only favorite child equipment model entities, you can select the Show Favorites toggle to switch it on. The Show Favorites toggle focuses your UI view on the child entities added to your favorites to help you stay on track while making changes in the Equipment Model Manager.

When you switch on the Show Favorites toggle, the configuration is saved. When you log out and log back in, or open a different site, the Show Favorites toggle is still switched on.

Automated Mapping Across Zone-based IP Network Groups

Automate mapping of Operational Technology (OT) devices to the production process using the Automated Mapping Across Zone-based IP Network Groups (AMAZING) feature.

When OT managers experience vulnerabilities or must manage workflow involving OT devices, the context of how the OT device connects to the production process it automates is critical to prioritizing work. Automatic mapping of OT devices to ISA equipment model entities enables the view of device-to-process relationships.

Note: Only one subnet range according to site is supported. Two different sites can have the same subnet; for example, 192.168.101.0/24. But multiple subnets of the same range are **not** supported for the same site. It is recommended that you use manual mapping in this scenario.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key benefits

- Upload and store OT subnets from authoritative sources (such as NetDB or Firewalls) as records in a ServiceNow instance.
- Automate assignment of OT devices to ISA entity using IP addresses and OT subnet.
- Minimize issues with reuse of private IP address ranges across multiple sites.
- Use discovered subnets in copy-paste networks to help uniquely identify OT devices for mapping.

Industrial networks use subnets to divide private IP address space, with each subnet aligned to a production process or equipment entity. For example, a canning line runs on a 192.168.101.0/24 network where all equipment was programmed by the integrator. IPs for control systems and OT devices are hard-coded into the automation software. When the subnet maps to a canning line in the Atlanta site, detected PLCs with IPs like 192.168.101.66 are automatically mapped to that line.

The mapping feature relates each subnet to an equipment model entity. You can map OT devices to associated subnets based on imported IP addresses from OT-certified integrations or Discovery for Operational Technology.

Types of mapping

The following types of mapping are supported in the AMAZING feature.

AMAZING mapping types

Type	Description
IP Network	Subset of IP addresses in a subnet. **Note:** IP network mapping isn't supported in a copy-paste network.
IP Range	Entire subnet, in CIDR notation **Note:** IP range mapping isn't supported in a copy-paste network.
Discovered Subnet	Discovered subnet in your OT network. **Note:** Discovered subnet mapping is supported in a copy-paste network.

Using discovered subnets to uniquely identify devices

Copy-paste networks create difficulty uniquely identifying OT devices and mapping them to equipment model entities. At some sites, the same IP subnet range applies to multiple equipment model entities, causing ambiguity about device mapping. Configure the discovered subnet to identify unique devices and their equipment model entities for more accurate mapping. By using discovered subnets with the AMAZING feature, you can uniquely identify OT devices in a copy-paste network. The logic is as follows:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. When OT device data is populated from a Service Graph Connector, the subnet and managed network must be populated in the IP Address [cmdb_ci_ip_address] table using the **Netmask** and **Network partition identifier** fields. The **Network partition identifier** field is important to the mapping process because it's always unique to an OT device.
2. The **Discovered subnet** and **Managed network** fields must also be populated in the OT device data for mapping to continue.

The AMAZING feature retrieves all configuration items (CIs) associated with a particular site. The IP address details, including the **Netmask** and **Network partition ID** fields, are obtained. Using the IP address details, the feature determines the discovered subnet then checks if the selected subnet and the managed network match the discovered subnet. If a match is found, the **Automated by :: Automates** relationship is established between the CI and the equipment model entity to effectively map the OT device to the correct entity.

The discovered subnets live in the OT Discovered Subnets [sn_ot_discovered_subnet] table available with the Industrial Core. This table leverages the following attributes to help refine OT device mapping accuracy:

- CIDR
- Discovered Managed Network
- Site

For more information about Industrial Core, see Industrial Core plugin.

You can also manually create a discovered subnet. For more information, see the Create an OT discovered subnet.

Automated mapping feature personas

The automated mapping feature is aimed at the following personas.

Personas for automated mapping

Persona	Description
System Admin	The System Administrator performs these tasks: • Imports data into the OT subnet to Equipment Model Entity Mapping table • Activates, schedules, or manually triggers the OT Subnet Mapping scheduled flow
ISA Admin	The ISA admin manually triggers the Map all OT devices UI action from the OT Subnet Mapping list view.
ISA Editor	The ISA editor performs these tasks:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Personas for automated mapping (continued)

Persona	Description
	• Manually creates and updates OT subnet mapping entries for specific sites • Maps individual OT devices to an equipment model entity from an OT device record • Maps multiple OT devices to an equipment model entity from an OT subnet mapping record

Plugins

Enabling the mapping feature requires the following plugins:

- Operational Technology Manager
- Industrial Process Manager
- Industrial Core

If the required plugins are installed, an ISA administrator can access the subnet mapping feature from the Industrial Process Manager application menu on the ServiceNow AI Platform.

Workflow for the automated mapping feature

The Industrial Process Manager includes an automated flow for the automated mapping feature.

A predefined flows is included with this feature that you can use to schedule the assignment of OT devices to equipment model entities.

By using Flow Designer, you can review and configure the predefined flow for your business needs.

Flow available for this feature

The following table lists the predefined flow that is available with the Industrial Process Manager when installed with Operational Technology Manager.

Application	Flow
Industrial Process Manager when installed with Operational Technology Manager	OT device mapping flow

General use cases for the automated mapping feature

These use cases typically apply for the automated mapping feature:

- An OT manager has existing OT devices and wants to map individual OT devices on demand.
- An OT admin wants to automatically map newly detected OT devices with valid IP addresses to an equipment model entity.

The following is a typical workflow for the automated mapping feature.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- A system admin imports OT subnet data into the OT subnet mapping table from an Excel spreadsheet using Easy Import.
- Either the Amazing admin reviews the imported data records and associates (maps) OT subnet mapping records to a site and/or the Equipment Model Entity within that site.
- The Amazing admin activates or triggers the scheduled flow to automatically map OT devices for all sites on an instance.
- The Amazing editor can update the records that belong to the sites that they have editing access to.

Configure Automated Mapping of OT devices using guided setup

Use the Industrial Process Manager guided setup to automatically map OT devices to the ISA equipment model entity.

Before you begin

Role required: admin

About this task

If you have the admin role, you can use the Industrial Process Manager Guided Setup to walk you through mapping OT devices to the ISA equipment model entity. You can map OT devices for the sites that you have access to.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup**.
2. Select **Get Started** for the Industrial Process Manager application.
3. Select the **Automatically Map OT Devices** task.
4. Select the following task tabs, then select **Configure** to complete the configuration tasks.

Task	Purpose
Import OT Subnets	Upload a spreadsheet of OT subnets to im port subnets from network management plat forms.
Add Sites	Add a site to each OT subnet so that OT de vices with IP addresses matched with the OT subnet record can be mapped to that site au tomatically.
Add Equipment Model Entities	Add an equipment model entity to the OT sub net record to automatically associate an OT device with the equipment model entity.
Select Discovery Source(s)	Configure the following OT subnet-map ping system properties to limit the discovery sources that OT subnet mapping considers. ○ sn_otsm.map_all_ot_devices.all_discov ery_sources ○ sn_otsm.map_all_ot_devices.discovery_ sources
Test Mappings	Validate assigned mappings of individual OT devices, individual OT subnets, multiple se lected OT subnets, or all active OT subnets.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Purpose
Activate and Schedule	Activate the scheduled flows to run sched uled mapping of all OT devices regularly. There are two subflows that you can trigger in dividually: ○ Subflow to assign sites to OT devices ○ subflow to map OT devices to a site

Related topics

Guided Setup

Automated Mapping Across Zone-based IP Network Groups

Configure the OT Subnet Mapping scheduled flow

Configure the OT device mapping flow to automatically map OT devices to sites and equipment model entities.

Before you begin

The following plugins must be installed:

- Operational Technology Manager
- Industrial Process Manager

Role required: admin

About this task

The OT device mapping flow can be set to run on a scheduled basis to automatically map OT devices for all active OT subnet mapping records.

Procedure

1. Navigate to **Industrial Workspace Admin** > **Industrial Process Manager** > **OT Subnet Mapping Scheduled Flow**.
2. **Optional:** Activate site mapping:
   a. Open the Set Flow Variables section.
   b. Check the box next to **Run Auto Assign Site** and select **Save**.
3. To schedule the flow to run on a regular basis, select the link in the Trigger section to define the interval.
4. In the header, select **Activate** to activate the scheduled execution of the OT device mapping flow.
   After activation, this flow can run on a scheduled basis to automatically map OT devices for all active OT subnet mapping records on an instance.

> **Note:** Subnet mapping also supports Discovery created configuration items (CIs) for ISA equipment models.

Automatically map all OT devices to an equipment model entity

An Operational Technology (OT) Amazing admin can trigger automated mapping of all OT devices to the appropriate ISA equipment model entity.

Before you begin

The following plugins must be installed:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Operational Technology Manager
- Industrial Process Manager

Role required: sn_ot_amazing_admin

Procedure

1. Navigate to **Industrial Workspace Admin** > **Industrial Process Manager** > **OT Subnet Mapping**.
2. Select **Map all OT devices** to execute the Map OT Device flow.

Result

OT devices are automatically mapped to the Equipment Model Entities listed on all active OT subnet mapping records. After the mapping is triggered, you can view the mapping results by selecting the link available in the information message from the list view.

Note: Subnet mapping also supports Discovery created configuration items (CIs) for ISA equipment models.

Create a new OT subnet mapping record

Create a new OT subnet mapping to associate with an equipment model entity.

Before you begin

Role required: sn_ot_amazing_write or sn_ot_amazing_admin

Note: When creating new OT subnet mapping records, by default the new records are inactive. To automatically map records when the OT device mapping flow triggers, OT subnet mapping records must be active.

Procedure

1. Navigate to **All** > **Equipment Model - ISA** > **Equipment Model Entities**.
   Alternatively, you can navigate to **All** > **Industrial Workspace Admin** > **OT Subnet Mapping**. Then select **New** in the OT Subnet Mappings table. If you create an OT subnet mapping record using this method, continue from step 4.
2. Select the site or equipment model entity you want to create a new mapping for.

   Note: Subnet mapping also supports Discovery created configuration items (CIs) for ISA equipment models.

3. Select the **Mapped OT Subnets** related list, then select **New**.
4. On the form, fill in the fields.

OT Subnet to Equipment Model Entity Mapping form

Field	Description
Name	Zone or VLAN name for the subnet.
Site	From the Lookup, select the ISA site from the list of available sites if not already populated.
Type	Select the subnet type from these options:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	• IP Range - a subset of IP addresses in a subnet • IP Network - the entire subnet, in CIDR notation • Discovered Subnet - a discovered subnet in your OT network
Discovered subnet	Reference to the OT Discovered Subnet [sn_ot_discovered_subnet] table. This field only appears if you select Discovered Subnet for the **Type** field.
Starting IP Address	Starting IP for the IP Range This field is visible when Type is IP Range.
Ending IP address	Ending IP for the IP Range This field is visible when Type is IP Range.
Source name	Name of the source, such as NetDB or Firewall.
Firewall Name	Name of the firewall managing the zone if applicable.
Description	Description for the subnet mapping.
Active	Select Active to include the subnet in automated mapping when the OT Subnet Mapping scheduled flow executes.
Equipment model entity	From the Lookup, select the equipment model entity from the list of available entities if not already populated.
Subnet	Enter the subnet address (CIDR format). This field is visible when Type is IP Network.
Location	Add a location to the subnet record to automatically add or update the location in the mapped OT devices. **Note:** The location is mapped based on the sn_otsm.subnet_mapping.location_auto_update system property. For more information about system properties used for OT subnet mapping, see System properties used by the OT subnet mapping feature.
Interface name	Name for the firewall interface if applicable.
VLAN ID	Specify the VLAN ID if applicable.

5. Select **Submit**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Map all OT devices within a subnet

An OT admin can trigger automated mapping of all OT devices within a selected subnet.

Before you begin

The following plugins must be installed:

- Operational Technology Manager
- Industrial Process Manager

Role required: sn_ot_amazing_write

Procedure

1. Navigate to **Industrial Workspace Admin** > **Industrial Process Manager** > **OT Subnet Mapping**.
2. From the OT Subnet Mapping list, open the OT subnet mapping record whose devices you want to map.

   Note: Subnet mapping also supports Discovery created configuration items (CIs) for ISA equipment models.

3. Ensure that the Site and Equipment Model Entity fields are correctly completed.
4. Select the **Map OT devices in this subnet** UI Action to automatically map all OT devices in this site with IP addresses in the selected OT subnet.

Result

If there are OT devices in the selected site with IP addresses that fall in the selected IP range, all devices in the site are mapped for the OT subnet. After the mapping is triggered, you can view the mapping results by selecting the link available in the information message from the list view.

Map OT devices to equipment model entities from the Equipment Model Manager

Map Operational Technology (OT) devices to equipment model entities from the Equipment Model Manager in the Industrial Workspace.

Before you begin

Role required: cmdb_ot_isa_editor and cmdb_ot_viewer

Procedure

1. Navigate to the Industrial Workspace.
2. To open the Equipment Model Manager, select the **Equipment model**  icon.
3. Select the equipment model entity that contains the OT devices you want to map.
4. In the equipment model entity record, select the **Mapped OT Devices** tab.
5. Select the **Map OT devices** UI action.
6. Using the **All devices** and **Unmapped devices** tabs, select the OT devices you want to map by clicking the check box in the first table column.
   The **All devices** tab shows all the OT devices available in your OT system, mapped or unmapped. The **Unmapped devices** tab shows the OT devices that aren't yet mapped to an equipment model entity. Using these 2 tabs to select OT devices gives you better visibility into which OT devices still need to be mapped to an equipment model entity.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the **All devices** tab, you can view the equipment model entities a device is already mapped to with the **Mapped Equipment Model Entity** column. In the **Unmapped devices** tab, the column is empty to show the device isn't mapped yet.

7. Select **Map devices**.
8. In the **Select equipment model entity to map devices** model, select the check box next to the equipment model entity or entities you want to map the devices to.
9. Select **Confirm**.

Result
Once you select **Confirm**, a message appears to notify you that the selected OT devices are being mapped and that the process may take a few minutes to complete.

What to do next
To view the newly mapped devices, you can select the link provided in the message. The link takes you back to the equipment model entity record. You can then open the **Mapped OT devices** tab to see the devices added to the list.

Map an individual OT device to an equipment model entity

Perform on-demand mapping of an OT device to the ISA equipment model entity for the sites that you have access to.

Before you begin
The following plugins must be installed:

- Operational Technology Manager
- Industrial Process Manager

Role required: sn_ot_amazing_write and cmdb_ot_viewer

Procedure
1. Navigate to the Industrial Workspace.
2. Open the Industrial Workspace list view.
3. Under the **Operational Technology (OT)** list module, select one of the available lists.
4. Select the OT device that you want to map.
5. In the OT device record, select the **More actions** ... icon.
6. Select the **Map OT device** UI action.

Result
If there is an active OT subnet that matches the IP address and site of the selected device, the device is mapped.

Create an OT discovered subnet

Create an Operational Technology (OT) discovered subnet to use during OT subnet mapping to help identify OT devices and assign them to the correct equipment model entity.

Before you begin
Role required: cmdb_ot_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **OT Discovered Subnets**.
2. Select **New**.
3. On the form, fill in the fields.

OT Discovered Subnet fields

Field	Description
CIDR	Classless Inter-Domain Range (CIDR) to identify IP addresses for the discovered subnet.
Discovered Managed Network	Name of the discovered managed network that the OT device belongs to.
Site	Site that the OT device belongs to.

Note: The combination of CIDR, Discovered Managed Network, and Site should always be unique so that the OT devices are correctly mapped to the equipment model entities.

4. Select **Submit**.
5. To edit the discovered subnet record, open the record, make the changes as needed, and select **Update**.

View OT devices not assigned to a site

View the list of Operational Technology (OT) devices that aren't assigned to a site.

Before you begin

The following plugins must be installed:

- Operational Technology Manager
- Industrial Process Manager

Role required: cmdb_ot_isa_editor and cmdb_ot_editor

About this task

As part of OT device mapping, you need to assign the device to a site before mapping it to an equipment model entity. To do this, you can view a list of all the OT devices that aren't assigned to a site.

Procedure

1. Navigate to **All** > **Operational Technology (OT)** > **OT Devices w/o Site Assignment**.
2. To assign a device to a site individually, select the device record and updating the **Site** field.
3. To perform a bulk edit to update the **Site** column and assign multiple devices to the same site, complete the following steps.
   a. Select the check boxes next to each OT device you want to assign to a site.
   b. In the **Site** column header, select the Column options button and choose **Update Selected**.
   c. Update the **Site** field.
   d. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next

The OT devices are assigned to a site but not mapped to an equipment model entity. You can view a list of the unmapped OT devices to complete the device mapping. For more information, see View unmapped OT devices.

View unmapped OT devices

View a list of Operational Technology (OT) devices with IP addresses that aren't mapped to any equipment model entity.

Before you begin

The following plugins must be installed:

- Operational Technology Manager
- Industrial Process Manager

Role required: cmdb_ot_isa_editor and cmdb_ot_editor

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the Industrial Workspace list view under the **Operational Technology (OT)** module, select the **Unmapped OT Devices** list.
   This list shows the OT device records with IP addresses and other fields that you can use to map them to equipment model entities for your assigned site.
3. **Optional:** In the **Site** column header, select the Filter button and choose **Group by Site**.
   This filter lets you organize the unmapped OT devices by site and can be helpful if you manage multiple sites.

What to do next

Now, you can map the OT devices to equipment model entities. For more information, see Map an individual OT device to an equipment model entity.

View OT subnet mappings

View all mapped OT subnets assigned to an equipment model entity.

Before you begin

Roles required:

- sn_ot_amazing_write, cmdb_ot_isa_editor, and cmdb_ot_viewer or
- sn_ot_amazing_admin, cmdb_ot_isa_editor, and cmdb_ot_viewer

Procedure

1. Navigate to the Equipment Model Manager using one of these options:
   - Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Equipment Model Manager**.
   - Navigate to **All** > **Industrial Workspace**. Select the Equipment model () icon.
2. From the Equipment model view, select the site, or expand the equipment model hierarchy to select the entity that you want to view mappings for.
3. In the entity form, select the **Mapped OT subnets** related list tab.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The mapped OT subnets show as active or inactive. Only active OT subnets will be included in the scheduled flow. For more information, see Configure the OT Subnet Mapping scheduled flow.

4. **Optional:** To view the OT subnets that are used for mapping at the OT device level, select the **OT Subnets** related list in an OT device record.

What to do next
Create a new OT subnet mapping record

View all mapped OT devices

View a list of all the Operational Technology (OT) devices that are mapped to an equipment model entity.

Before you begin
Role required: sn_ot_amazing_write or sn_ot_amazing_admin

About this task
When you open a parent record in the CI Relationships table, you can view the Mapped OT Devices related list. The related list is a rolled up view that shows all the devices mapped with children ISA equipment model entities after you open the parent ISA equipment model entity. It contains the records that represent a mapping between an equipment model entity and a device.

Procedure
1. To view the mapped OT devices in the Industrial Workspace, complete the following actions.
   a. Navigate to the Industrial Workspace.
   b. Select the Equipment model ( ) icon.
   c. Open the equipment model entity that you want to view the mapped devices for.
   d. Select the **Mapped OT Devices** tab.

   Note: The **Mapped Equipment Model Entity** column notes the equipment model entity that the device is mapped to. You can map a device to more than one equipment model entity.

2. To view the mapped OT devices on the ServiceNow AI Platform, navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Mapped OT Devices**.
   This list contains all the devices that are mapped with different equipment model entities. The **Automates by :: Automates** CI relationship is applied to the parent and child entities.

   In this list, you can use the **Mapped Equipment Model Entity** column to identify the equipment model entity the device is mapped to. For more information on how to add a column to a list, see Personalize a list.

Industrial Process Manager reference

Reference topics provide additional information about the Industrial Process Manager application.

Components installed with Industrial Process Manager

Several types of components may be installed with activation of the Industrial Process Manager application, including user roles.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Roles installed

Role	Description
Equipment Model Viewer [cmdb_ot_isa_viewer]	Can only view the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] table records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models.
Equipment Model Editor [cmdb_ot_isa_editor]	Can view and edit the assigned ISA Equipment Model [cmdb_ci_ot_isa_entity] records. To learn more, see Using Industrial Process Manager with the Operational Technology Manager and Managing equipment models.
Equipment Model Admin [cmdb_ot_isa_admin]	Inherit the cmdb_ot_isa_editor role and can also do the following actions: • Use the Industrial Guided Setup to set up the Industrial Process Manager and the Operational Technology Manager. • Edit the Equipment Model Template [isa_entity_template], [isa_entity_level], and Equipment Entity type [isa_entity_type] table records. To learn more, see Industrial Workspace Admin application menu and Guided Setup.
ISA Site Viewer [cmdb_ot_isa_bypass_qbr]	Can view all sites in the OT Progress Scorecard.
Equipment Model Downtime Planner [sn_isa_schedule_admin]	Can create, modify, and delete equipment entity schedules. Can also associate schedules with equipment entities.
Equipment Model Viewer All [cmdb_ot_isa_viewer_all]	Can view all ISA Equipment Model records (cmdb_ci_ot_isa_entity) and associated Equipment Model Template records (isa_entity_template, isa_entity_level, isa_entity_type). Role included with cmdb_ot_admin.
Amazing Admin [sn_ot_amazing_admin]	Can create, modify and delete OT subnet records (ot_subnet_mapping) for all the equipment model entity OT subnet system properties.
Amazing Editor [sn_ot_amazing_write]	Can create, modify and delete OT subnet records (ot_subnet_mapping) for all the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role	Description
	equipment model entities associated with the user.
Amazing Viewer [sn_ot_amazing_read]	Can view OT subnet records (ot_subnet_mapping) for all the equipment model entities.

ISA Equipment Model system properties

Enable the system properties for the ISA Equipment Model as needed.

You can access the system properties for the ISA Equipment Model by navigating to **All** > **Industrial Workspace Admin** > **All OT Properties**. For more information about how to view and edit the OT system properties, see View and edit OT system properties.

The following table describes the system properties for the ISA Equipment Model.

ISA Equipment Model System Properties

System property	Description	Type
sn_isa_model.cmdb_relationships_sync_levels	Number of levels of CMDB relationships that are synchronized.	Integer
sn_isa_model.short_code_validation_max_length	Maximum length for the short code validation.	Integer
sn_isa_model.excluded_operational_statuses	List of equipment model operational statuses that need to be filtered out from the equipment model page.	String
sn_isa_model.user_search_matching_attribute	Column in the User Table [sys_user] that matches with a user in the system. By default, the Email column on the User table is used.	String
sn_isa_model.user_sites_cache_expiration_time	Expiration time in seconds. The default is set to 600 (10 minutes).	Integer
sn_isa_model.use_user_sites_cache	Enables the session cache for ISA entity records.	Boolean
sn_isa_model.isa_entity.validate_and_generate_location	Allows display of the **Auto generate location** UI action (UI16 and Workspace) and the **Location Validation Map** tab (Workspace) in the Equipment Model form. Validates synchronization between the ISA Equipment Model Entity Hierarchy and its referenced CMN Location Hierarchy.	Boolean

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ISA Equipment Model System Properties (continued)

System property	Description	Type
	Automatically creates CMN Location records for each new ISA entity within the ISA Hierarchy, connecting them to the CMN Location Hierarchy. The default is set to false.	

System properties used by the OT subnet mapping feature

An Amazing Admin can view and configure the system properties that support the OT subnet mapping feature.

Users with the Amazing Admin role can access OT subnet mapping property settings by navigating to **Industrial Workspace Admin** > **Industrial Process Manager** > **OT Subnet Mapping Properties**.

OT subnet mapping system properties

Property	Description
sn_otsm.map_all_ot_assets.all_discovery_sources	Map OT devices for all discovery sources. Map OT devices for all discovery sources. If checked, this will override the specific discovery sources below. Default is Yes (true). Default value: **true**
sn_otsm.map_all_ot_assets.discovery_sources	Map OT devices for specified discovery sources (comma separated format). Only applicable if "Map OT devices for all discovery sources" above is unchecked.
sn_otsm.subnet_mapping.auto_assign_all_OTs	Automatically assign all OT control modules to equipment model entities based on the Owns::Owned by relationship. Default is Yes (true).
sn_otsm.subnet_mapping.location_override	Override location of an OT device with subnet's location. If checked, the location of the subnet takes precedence over OT device's location when it's mapped with the subnet. Default is Yes.

Automated mapping components installed when Industrial Process Manager and Operational Technology Manager are both installed

Several types of automated mapping components will be installed with activation of the Industrial Process Manager when Operational Technology Manager is also active, including tables, system properties, and scheduled flows.

These automated mapping components are installed with or available when Industrial Process Manager is installed with Operational Technology Manager.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tables

Table	Description
OT Subnet to Equipment Model Entity Mapping [ot_subnet_mapping]	Stores the mappings of OT subnet to equipment model entities.

Properties

Property	Description
sn_otsm.map_all_ot_assets.all_discovery_sources	Control mapping of OT devices for all discovery sources. Default value: **true**
sn_otsm.map_all_ot_assets.discovery_sources	Map OT devices for specified discovery sources (comma separated format).
sn_otsm.subnet_mapping.auto_assign_ot_control_modules	Automatically assigns all OT control modules to equipment model entities based on the Owns::Owned by relationship. Default is Yes (true).
sn_otsm.subnet_mapping.location_auto_update	Override location of an OT device with subnet's location. If checked, the location of the subnet takes precedence over OT device's location when it's mapped with the subnet. Default is Yes.

Flow Designer flows

Application	Flow
Industrial Process Manager integration with Operational Technology Manager	OT device mapping flow

Migrating site user access to user criteria and groups

When you upgrade to version 1.0.12 of the ISA Equipment Model, the migration from site user access to user criteria and groups begins automatically.

The following changes occur when you upgrade to version 1.0.12 of the ISA Equipment Model.

- Improved site level access control that uses user criteria to define read or write level user access to equipment model entity sites. Assign the OT viewer (cmdb_ot_viewer) or OT Editor (cmdb_ot_editor) role to have view or edit access to OT devices in the assigned sites.
- When you upgrade to version 1.0.12 of ISA Equipment Model, existing site user records are migrated to an improved access control model using user criteria to preserve the same access permissions. For each site with ISA Entity Site User records, the following changes occur.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For users with viewer access:
  - A new user criteria record is created and named **Read User Criteria for <site name> Site#[System Generated]**
  - A new user group with all site users from this site is created and named **Read Group for <site name> Site [System Generated]**
  - A new record in the new Equipment Model Entity View Access table (isa_entity_m2m_user_criteria_can_view) is created with the new user criteria and user group.
- For users with editor access:
  - A new user criteria record is created and named **Edit User Criteria for <site name> Site [System Generated]**
  - A new user group with all site users from this site is created and named **Edit Group for <site name> Site [System Generated]**
  - A new record in the new Equipment Model Entity Edit Access table (isa_entity_m2m_user_criteria_can_edit) is created with the new user criteria and user group.

- The Site User application menu and Site Users related list on the Equipment Model Entity record for a site is removed.
- All site user (isa_entity_site_user) records are set to inactive.
- The **Site User – Can Read** and **Site User – Can Edit** application menu items are added to the ServiceNow AI Platform.
- The **Can Read Equipment Models** and **Can Edit Equipment Models** related lists are added to the Equipment Model Entity record for a site.

User criteria form

You can use the User Criteria form to determine whether certain users can access the equipment model entities for specific sites.

The following table describes the user criteria form fields.

User criteria form

Field	Description
Name	Name of the user criteria.
Short description	Brief description of the user criteria to access the site's equipment model entities.
Users	Users that can access the site's equipment model entities when you apply the user criteria. Select the users who can access the entities by selecting the unlock users icon ( ). Add yourself as a user by selecting the add me icon ( ).
Groups	Groups that can access the site's equipment model entities when you apply the user criteria. Select the groups by selecting the unlock groups icon ( ).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

User criteria form (continued)

Field	Description
Roles	Roles that can access the site's equipment model entities when you apply the user criteria. Select the groups by selecting the unlock groups icon ( ).
Advanced	Option to create a script for the user criteria.
Application	Field that is automatically set to `Global`.
Active	Option to make the user criteria available.
Companies	Companies that can access the site's equipment model entities when you apply the user criteria. Select the companies by selecting the unlock companies icon ( ).
Locations	Locations that can access the site's equipment model entities when you apply the user criteria. Select the locations by selecting the unlock locations icon ( ).
Departments	Departments that can access the site's equipment model entities when you apply the user criteria. Select the departments by selecting the unlock departments icon ( ).
Match All	Option to make every condition required when the user criteria are applied. The conditions are set in the previous fields, such as the **Location**, **Department** fields.

Predefined filters for the Industrial Process Manager

Industrial Process Manager application uses predefined filters so that you can view the equipment model dependency maps by selecting the available UI actions in the Industrial Workspace.

The following predefined filters are available for the Industrial Process Manager.

ISA Equipment Model - Hierarchy Process

The hierarchical structure of the selected equipment model entity and its relationships to other entities in the production process.

ISA Equipment Model - OT Dependency Map

The hierarchical structure of the selected equipment model entity and its relationship with other entities and Operational Technology (OT devices in the production process.

ISA Equipment Model - OT Device Map

The graphical representation of the selected equipment model entity and its relationship to other OT devices in the production process.

ISA Equipment Model - Process

The graphical representation of the selected equipment model entity and its relationship to the production process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can view the equipment model dependency maps using the described predefined filters by navigating to the **Industrial Workspace** and opening the equipment model view. Then you can select the equipment model entity you want to view a dependency map for. When you open the record, you see the following UI actions to choose from:

- View OT Dependency map

  Note: You can also view the OT Dependency map in an OT device record by selecting **View map** in the record header.

- View OT Device map
- View hierarchy
- View process

You can also update the predefined filters as needed for your organization. For more information, see Modify predefined filters.

Modify predefined filters

Modify the predefined filters for the ISA Equipment Model application as needed for your organization.

Before you begin

Role required: ecmdb_admin

Procedure

1. Navigate to **All** > **Dependency Views** > **Predefined Filters**.
2. Apply the filter **[Application] [is] [ISA Equipment Model]**.
3. Select the predefined filter record that you want to edit.
4. Modify the Configuration Types, CI Filters, and Relationship Types related lists as needed. For more information about how to modify these related lists, see Create a predefined filter.
5. Select **Update**.

Site vs location

The site and location attributes have different uses for Operational Technology (OT).

Site

A site is part of the ISA Equipment Model Entity and describes an industrial site where your production process takes place. Sites are logical and you can use them to define an equipment model. You can then use that equipment model to provide access control. For more information about access control, see Manage equipment model site access for non-administrators.

Sites can have a location but they aren't considered a location. Any OT device can have a location and be assigned to an equipment model entity site.

Location

Location refers to the value stored in the **Locations** (cmn_location) table. It's the physical location of an equipment model or device. For example, if one of your equipment models belongs to the site Atlanta and is located in Atlanta, GA, you would list its location as **Atlanta, GA**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related information

Find more information about the Network Intrusion Detection System (NIDS) extension class, OT extension classes, and related applications.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Network Intrusion Detection System (NIDS) CI extension class

The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.

Operational Technology (OT) extension classes

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

Operational Technology Manager

The Operational Technology Manager application enables you to aggregate OT device data from multiple sources, so that you can build the foundational data relationships used in the Industrial solution.

Operational Technology Vulnerability Response

Operational Technology Vulnerability Response enables effective prioritization and remediation of OT device vulnerabilities at the site level. By leveraging the CMDB relationships of OT devices, vulnerable devices or items can be prioritized based on the criticality of the production process they automate.

Explore  Exploring Operational Technology Vulnerability Response	Configure  Configuring Operational Technology Vulnerability Response
Use  Using Operational Technology Vulnerability Response	Integrate  Extend Operational Technology Vulnerability Response by integrating it with other applications

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Reference



Get details about related information and applications

Exploring Operational Technology Vulnerability Response

Use Operational Technology Vulnerability Response as an integrated solution for the industrial production process.

Operational Technology Vulnerability Response overview

https://player.vimeo.com/video/1020858131?h=c90c2ff89a&badge=0&autopause=0&player_id=0&app_id=58479

As an OT engineer or OT vulnerability manager, Operational Technology Vulnerability Response enables you to find answers to the questions such as:

- What are my OT device vulnerabilities?
- How can I prioritize vulnerability remediation using OT specific risk?
- What progress are we making toward remediating OT vulnerabilities?

Remediation task and vulnerable item states

Vulnerable items (VITs) and their remediation tasks can have different states due to complex use cases. For more information about remediation task and vulnerable item states and their workflow, see Vulnerability Response remediation task and vulnerable item states.

Key features

With Operational Technology Vulnerability Response, you can use the following key features.

- The Operational Technology Vulnerability Response (PA) dashboard tracks the volume, performance, and progress of OT VITs from initial analysis and detection to containment, or remediation.
- The Operational Technology (OT) Vulnerability Risk Rollup dashboard contains the risk score of the OT devices at each level of the equipment model.

Operational Technology Vulnerability Solution Management

Starting from the Xanadu version, Operational Technology (OT) Vulnerability Solution Management is a feature available within the Operational Technology Vulnerability Response application.

Security and IT teams often spend a significant amount of time and effort to research vulnerability findings and identify the most effective solutions for their environment. In large organizations, translating vulnerability findings into remediation tasks is a manual, tedious, and error-prone process due to the volume and complexity of the vulnerabilities.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Vulnerability Solution Management automatically correlates the vulnerability findings in your environment with possible solutions that remediate them. You can identify the remediation actions that apply to your vulnerabilities and prioritize them by the severity of the vulnerability risk. Also, you can mitigate the risk posed by vulnerabilities that cannot be patched immediately by using compensating controls for OT. For more information, see Use compensating controls for Operational Technology.

The OT Vulnerability Solution Management feature is based on the feature available in the Vulnerability Response application. For more information on Vulnerability Solution management, refer to Vulnerability Solution Management.

OT Vulnerability Solution Management supports the generic format for solution intelligence integration. The generic framework for solution intelligence integration ingests data in different file formats from solution vendors. These formats speed up information exchange and processing. It also improves critical security-related information sharing in a standardized reporting format. The supported file format is the Common Security Advisory Framework (CSAF), which is an open-source standard that provides JSON-based structured, machine-readable security advisories. Major vendors such as Cybersecurity & Infrastructure Security Agency (CISA), Siemens, Hitachi, Schneider Electric, and others support the CSAF format.

The CSAF supported solution management includes the following key features:

- Configuration through Setup Assistant. For more information, see Configure vulnerability solution providers.
- Support of importing CSAF data through file import. For more information, see Import Common Security Advisory Framework data through file import.
- Support of importing CSAF data through CSAF URL. For more information, see Import Common Security Advisory Framework (CSAF) data through CSAF URL. OT Vulnerability Solution Management enables you to import CSAF data from:
  - Individual vendors that support CSAF format and have a CSAF URL ROLIE Feed. You can use the CSAF URL ROLIE Feed provided by the vendor to import the CSAF data. For example, the Siemens URL ROLIE Feed.
  - CSAF Aggregators or Trusted Providers through a URL import that supports the ROLIE Feed. You can import CSAF data of multiple vendors from a Trusted Provider. For example, CISA is a Trusted Provider and you can import CSAF data of multiple vendors from the Industrial Control System (ICS) CSAF advisories located at the CISA's GitHub CSAF repository. These vulnerability solutions are automatically mapped to the correct vendor and vulnerable items (VITs) based on the Common Vulnerabilities and Exposures (CVEs). Using a Trusted Provider reduces the time and effort required to import CSAF data from individual vendors' CSAF URLs.
- Support of importing CSAF data through advisories or using the APIs. For more information, see Import Common Security Advisory Framework data from advisories.

Note: Navigate to **All** > **Vulnerability Response** > **Solutions** > **All** to view the list of solutions you have imported using the preceding methods.

The Vulnerability Response plugin takes care of updating the metrics statuses of the created solution.

Related topics

View vulnerable items and solutions in the Industrial Workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuring Operational Technology Vulnerability Response

Configure Operational Technology (OT) assignment rules, remediation targets, risk calculators, and risk rollup calculation then configure integrations to create vulnerable item records.

Note:

If you have the sn_vul.vulnerability_admin role, you can use the Industrial Guided Setup to lead you through the setup of the Operational Technology Vulnerability Response application.

To access the Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

Task	Purpose
1. Install Operational Technology Vulnerability Response from the ServiceNow Store.	Install the Operational Technology Vulnerability Response application.
2. Assign roles to admin users#br user groups, if needed.	Assigns roles to control the actions that are available for each user.
3. Assign roles for the OT Vulnerability Remediation Owner.	Assigns roles to control the actions that are available for the OT Vulnerability Remediation Owner.
4. Create assignment groups and assign users to sites and groups. **1.** Create an Operational Technology Vulnerability Response site assignment group for each site that you have in the Equipment Model Manager. **2.** Assign users who already have either the cmdb_ot_isa_viewer or cmdb_ot_isa_editor role to sites. **3.** Add users to the assignment group for their site.	• Allows OT Remediation Owner users to see only vulnerable Items for their site. • Allows users to see the Vulnerability Items for the sites they're assigned to.
5. Configure OT remediation target rules.	• Assigns OT vulnerable items to site-level groups, or groups based on classification. • Defines the expected timeframe for remediating vulnerable items.
6. Load the demo data records for the Operational Technology Vulnerability Response application.	Calculates the remediation target for OT vulnerable items.
7. Configure OT risk calculators.	Determines which OT risk factors to use when calculating the risk of a vulnerable item on an OT device.
8. Configure OT risk roll up calculator.	Calculates the risk score of the OT devices at each level for the equipment model entity.
9. Install Operational Technology Certified integrations for the Operational Technology	Integrates certified third-party applications that enhance functionality of OT vulnerability management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	Purpose
Vulnerability Response application that are applicable to your environment.	

In tasks 5,7, and 8, the guided setup redirects you to the Security Exposure Management Workspace (SEM Workspace). The SEM Workspace is part of ServiceNow's next-generation platform, Unified Security Exposure Management (USEM). USEM consolidates multiple security exposure applications—Vulnerability Response (VR), Application Vulnerability Response (AVR), Container Vulnerability Response (CVR), and Configuration Compliance (CC)—into a unified architecture. It provides a single source of truth for security exposure, enabling real-time visibility, streamlined workflows, and automated remediation through the SEM Workspace. The SEM Workspace is available for Security Operations Vulnerability Response from version 30.0.0.

As Vulnerability Response is now consolidated under USEM, starting from Operational Technology Vulnerability Response version 2.0.0, users may be redirected to the SEM Workspace to perform some configuration tasks.

Install Operational Technology Vulnerability Response

Install the Operational Technology Vulnerability Response application if you have the admin role. This application includes demo data and installs the related store applications and plugins if they are not already installed.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- If the application requires plugins or other store applications, install them first if they are not already installed.
- Operational Technology Vulnerability Response requires the following plugins. Ensure that these plugins are activated before you install Operational Technology Vulnerability Response.

Required ServiceNow plugins

Vulnerability Response (sn_vul)

The ServiceNow® Vulnerability Response application imports and automatically groups vulnerable items according to group rules allowing you to remediate vulnerabilities. See Install Vulnerability Response

Industrial Process Manager (sn_otsm)

Creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Industrial solution. See Install the Industrial Process Manager.

Operational Technology Manager

The Operational Technology Manager application creates the foundational data and relationships that enable your enterprise to use the ServiceNow® Industrial solution. Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the ServiceNow AI Platform. See Configuring the Operational Technology Manager (OTM).

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The following items are installed with the installation of the Operational Technology Vulnerability Response application:

- Plugins
- Store applications
- Roles
- Business rules

For more information on viewing the components that are installed with an application, see the following:

- Components installed with Operational Technology Vulnerability Response
- Find components installed with an application.

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Operational Technology Vulnerability Response application using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find an application, you may have to request it from the ServiceNow Store.

   Visit the ServiceNow Store to view all the available apps, and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.
3. Select a version from the list and select **Install**.

   In the Review Installation Details dialog box, any dependencies installed with your application are listed.
4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. **Optional:** If demo data is available and you want to install it, select the **Load demo data** check box.
   Demo data are the sample records that describe application features for common use cases. Load the demo data when you first install the application on a development or test instance.
6. Select **Install**.

Assign Operational Technology Vulnerability Response roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Operational Technology Vulnerability Response application.

Before you begin

Role required: admin or user_admin

About this task

Users with the roles that are listed in the following tables can use the Operational Technology Vulnerability Response application.

Assign roles to admin users#br user groups as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign roles to admin users#or groups

Role	Description
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view OT VR integration records.
OT VR Integration Admin [sn_otvr.integration_admin]	Can view and edit OT VR integration records.
OT Vulnerability Remediation Owner [sn_otvr.remediation_owner]	Can create remediation tasks. Can also schedule existing remediation tasks for vulnerable items.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

What to do next

Create a site assignment group.

Create a site assignment group

Create one Operational Technology Vulnerability Response assignment group per site that you have in the Equipment Model Manager. This allows OT Remediation Owner users to only see vulnerable items for their site.

Before you begin

Create an Operational Technology Vulnerability Response assignment group, preferably with the same name as the site it will be related to. For example, if your site is in Milan, name the group the 'Milan OT VR Assignment Group'.

Role required: admin, or both cmdb_ot_isa_admin and user_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Industrial Process Manager** > **Sites**.
2. Select a site record.
   The site record is a parent Equipment Model Entity that has no parent itself.
3. In the **OT VR assignment group** field, select the search icon to show existing user groups.
4. Select the applicable assignment group.
   - If the desired group exists, select it from the list.
   - If the desired group does not exist, select **New** to create the group, then select **Submit**.
5. After returning to the site record, select **Update**.
   The new OT VR assignment group is created.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
Assign users to sites

Assign users to sites

If you have not already done so during configuration of the Industrial Process Manager, assign users who already have either the cmdb_ot_isa_viewer or cmdb_ot_isa_editor role to sites.

Before you begin
When OT devices are in the CMDB, site access can be configured to limit visibility of OT devices to users with both a cmdb_ot_viewer, editor, or admin role, and a cmdb_ot_isa_viewer or editor role.

Role required: admin or cmdb_ot_isa_admin

Procedure

1. From the Equipment Model Entities form, select a parent Equipment Model entity.
   For information about equipment models, see Managing equipment models.
2. From the Site Users tab, select **New**.
3. On the ISA Entity Sites Users form, fill in the fields.
4. Select **Submit**.
   The user is assigned to the site.

What to do next
Assign users to assignment groups

Assign users to assignment groups

Add users to assignment groups so they can see the vulnerability items for their assigned site.

Before you begin
To allow users to see the vulnerability items for the sites you've assigned them to, add users to the OT VR assignment group for the site.

When OT vulnerable items are created, visibility is limited to:

- Users with the VR Remediation Owner (sn_vul.remediation_owner) role
- Membership in the Operational Technology Vulnerability Response assignment group associated with the site that the OT device belongs to

Role required: admin or user_admin

Procedure

1. Open the group that corresponds to the Operational Technology Vulnerability Response assignment group for the site.
2. From the Group Members tab, select **Edit**.
3. Add the users from the Collection list into the Group Members List.
4. Select **Save**.
   Users are assigned to the group and can see the vulnerability items for the assigned site. For more information about admin tasks, such as adding users to groups, see User administration.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

What to do next
Assign vulnerable items to groups.

Assign vulnerable items to groups

Configure OT Vulnerability assignment rules.

Before you begin
OT Vulnerable Items can be assigned to site level groups or groups based on classification, depending on your remediation strategy.

Role required: sn_sec_wf.manage_admin_rules

About this task
When Vulnerable Items are imported, they are assigned to the appropriate group based on Vulnerability Assignment Rules. Operational Technology Vulnerability Response ships with one OT vulnerability assignment rule, **Operational Technology (OT) assignment rule**, which assigns OT vulnerable item records (VIT) to the corresponding OT VR assignment group based on its site. If it does not belong to any site, or if there's no group specified on the site, the rule assigns to the OT VR Default Assignment Group.

For more information about creating Vulnerability Response assignment rules, see Create or edit Vulnerability Response assignment rules.

Procedure
1. Navigate to **All** > **Industrial Workspace** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Assignment Rules** > **Configure**.
2. Alternatively, navigate to **Workspaces** > **Security Exposure Management** > **Administration** > **Assignment**.
3. In the Assignment list displayed in the Security Exposure Management Workspace, select **Operational Technology (OT) assignment rule**.
4. Configure it based on your remediation strategy:
   - If your remediation strategy is to assign all OT Vulnerable Items to the site, set the execution order of the OT VR Assignment rule to be less than all other rules.
   - If your strategy is to assign by class and then assign to sites for all other classes, set the execution order of the OT VR Assignment Rule to be greater than all class-based rules.
5. Once the execution order is updated, set the OT VR Assignment Rule Active state to **true**.

What to do next
Configure OT remediation target rules.

Configure OT remediation task rules

For remediation tasks that are created in the Industrial Workspace, update existing remediation task rules to prevent imported vulnerable items from automatically adding OT devices.

Before you begin
Role required: sn_sec_wf.manage_admin_rules

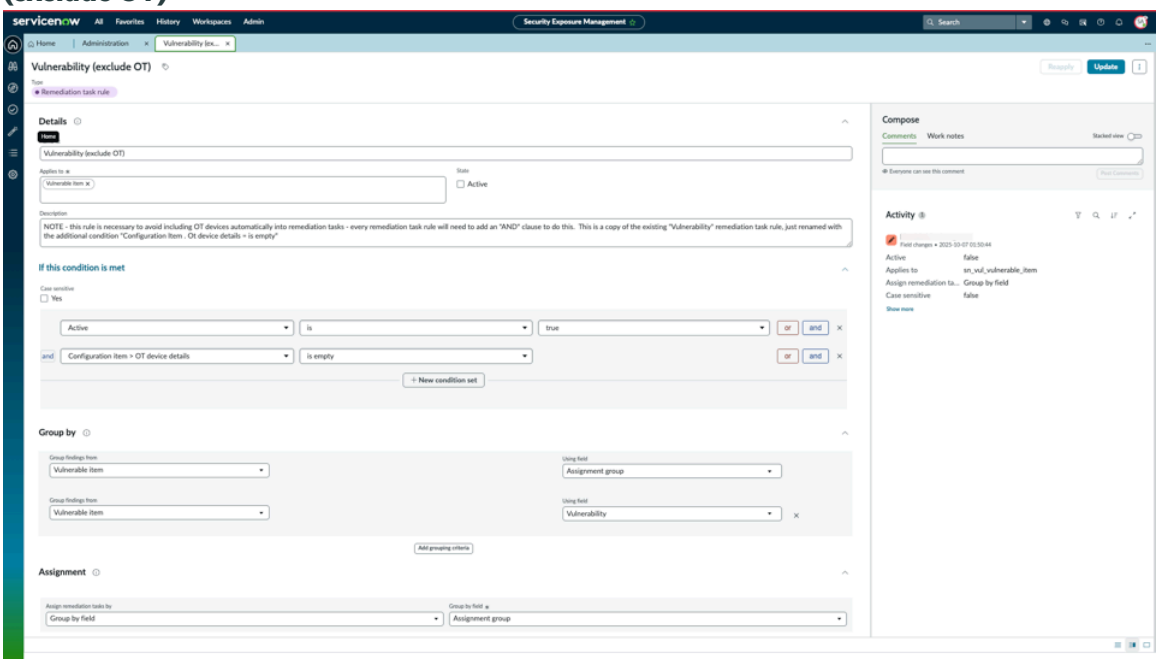
When vulnerable items are imported, they can be added to remediation tasks based on configured remediation task rules. If you use Vulnerability Response for both IT and OT networks, you must modify a configuration if you group Vulnerability Items for remediation differently between IT and OT networks. Operational Technology Vulnerability Response provides a sample Remediation Task Rule record that is loaded with demo data to demonstrate how to exclude OT network vulnerabilities from being grouped automatically.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configure any new or existing Remediation Task Rules based on your remediation strategy:

- If your remediation strategy is to automatically create remediation tasks only for vulnerabilities within your IT environment, add the following condition to each existing remediation task rule to exclude OT vulnerabilities:
  - Configuration Item . OT device details = **is empty**
- If your remediation strategy is to automatically create remediation tasks for all OT vulnerable items, create an appropriate rule.

Sample shipped with OT VR demo data: Remediation Task Rule - Vulnerability (exclude OT)



Procedure

1. Navigate to **All** > **Industrial Workspace** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Remediation Task Rules** > **Configure**.
2. Alternatively, navigate to **Workspaces** > **Security Exposure Management** > **Administration** > **Remediation Task**.
3. Select the name of the rule you want to update.
   - Define the rules such that all vulnerable items within a group are remediated by the same team, the same remediation action, and the same timeframe. For example, group by vulnerable item "Assignment group", "Vulnerability", and CI "Used for" (ex. Production, Staging, Development) if those environments have different maintenance windows.
   - For more information about remediation task rules, see Vulnerability Response Workspaces.
   - For more information about remediation tasks, see Explore the IT Remediation Workspace.

Configure OT remediation target rules

Configure remediation target rules for OT vulnerable items.

To calculate the remediation target date for OT vulnerable items, load the demo data records for the Operational Technology Vulnerability Response application and configure the remediation target rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role required: sn_sec_wf.manage_admin_rules

To configure OT Remediation Targets or load the demo data records:

- Navigate to **All** > **Industrial Workspace** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Remediation Targets** > **Configure**
- Or, navigate to **Workspaces** > **Security Exposure Management** > **Administration** > **Remediation target** > **Configure**.

OT Remediation Targets may be different due to the infrequent opportunities to perform maintenance in an industrial environment. Remediation target rules are applied in order from smallest target to largest target.

A different remediation target date may be needed for OT device vulnerabilities that do not have maintenance windows available in the same time frame as other vulnerabilities. To demonstrate how to configure remediation target dates in this situation, two demo data records are provided to demonstrate how this can be managed for Critical risk ratings:

- Critical Risk Rating rule (OT only) - This rule uses the condition of **Configuration item.OT device details is not empty AND Risk rating = 1- Critical**. Update the Target (days) and activate the record.
- Critical Risk Rating rule (exclude OT) - In order to apply a shorter target to Critical Risk non-OT items only, you need to filter out OT devices first. This rule uses the condition **Configuration item.OT device details is empty AND Risk rating = 1- Critical**. Update the Target (days), inactivate any existing critical target rule, and activate this rule in its place.

Note: Both of these rules must be activated so that any OT critical risk vulnerabilities are excluded from the non-OT remediation target rule.

For more information about creating Vulnerability Response assignment rules, see:

- Vulnerability Response remediation target rules
- Create or edit Vulnerability Response remediation target rules

Configure risk calculators

Configure risk calculators

Determine which OT risk factors to use when calculating the risk of a vulnerable item on an OT device.

Before you begin

In Operational Technology, additional factors can include the OT device criticality, the Purdue Level, and the criticality of the production process that the OT device automates.

Role required: sn_sec_wf.manage_admin_rules

About this task

For this step, refer to the Default Risk Calculator with OT vulnerability calculator shipped with the Operational Technology Vulnerability Response application. The Default Risk Calculator with OT is used when risk must be calculated differently for OT and non-OT vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note:

- You can directly access and use the Operational Technology Vulnerability Response Risk Calculator without loading the demo data while installing the plugin. In previous releases, Risk Calculation was included as part of the demo data.
- Because only one vulnerability calculator can be active at a time, the provided Default Risk Rule (non OT) is used as an example for calculating risk for all non-OT vulnerable items.

For more information, see Define fields and weights for the risk rule.

To set the risk score for OT vulnerable items, adjust the weights for the risk rule records of the OT Default Risk Rule in the demo data. More fields available for OT in the demo data include:

- Equipment Model Entity Criticality - Use the Service Business criticality rule.
- OT Device Criticality - Use the Configuration item OT device details Device Criticality rule.
- Purdue Level - Use the Configuration item OT device details Purdue level field.

Procedure

1. Navigate to **All** > **Industrial Workspace** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Vulnerability Risk Calculators** > **Configure**.
2. Alternatively, navigate to **Workspaces** > **Security Exposure Management** > **Administration** > **Risk Calculator**.
3. From the Risk Calculators list, select **Default Risk Calculator with OT**.
4. From the Risk Rules list, open the risk rule that you want to edit.
   For example, select **OT Default Risk Rule**.
5. In the Scoring Criteria section, select one or more risk rule field and update the weight or the weightage % for each criterion according to its importance in the overall risk score calculation.
6. Select **Update**.

What to do next

To set the risk score for all other vulnerable items, copy the existing risk rules to the Default Risk Calculator with OT, and set the order to run after the OT Default Risk Rule.

Configure OT vulnerability risk rollup calculator

Use the OT vulnerability risk rollup calculator to calculate the risk score of the OT devices at each level of the equipment model. The overall risk score is rolled up to the parent equipment model entity.

Before you begin

- Calculate the risk score for all the equipment model entities by executing the scheduled job.

  Note: The risk score calculation for all the equipment model entities is only for the subsequent run of the daily schedule job.

- Check that the Service Populator column in the Equipment Model Entities list is set to **OTDynamicManualServicePopulator** by navigating to **All** > **Equipment Model - ISA** > **Equipment Model Entities**. If it's set to other values, you must execute the *`Update ISA entity service populator`* on-demand job:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Navigate to **All** > **System Definition** > **Scheduled Jobs**.
- Select the *Update ISA entity service populator* job.
- Select **Execute Now**.

Note: If you don't see the Service Populator column in the Equipment Model Entities list, you can add it by personalizing the list. For more information, see Personalize a list.

- Role required: admin or sn_vul.manage_risk_score_configuration

About this task

For this step, refer to the Vulnerability Rollup Calculators with OT vulnerability calculator shipped with the Operational Technology Vulnerability Response application demo data.

For more information, see Vulnerability Response Rollup Calculators.

To calculate the risk score for the equipment model entity, set up the weights for these fields:

- Maximum risk score of the Vulnerable Items (VITs) associated to the equipment model entity.
- Average risk score of the VITs associated to the equipment model entity.
- Number of vulnerable items per equipment model entity.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Rollup Calculator**.
2. Navigate to **Workspaces** > **Security Exposure Management** > **Roll-up**.
3. From the Roll-up calculators list, select **Equipment Model Entity Rollup**.
4. If required, in the Roll-up weightage section, update the weight for each criterion.
5. Select **Update**.

What to do next

Now, you can calculate the risk associated at a level for your equipment model entities.

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > **Operational Technology Vulnerability Response** > **OT Vulnerabilities Dashboard Risk Rollup**.
2. Calculate the risk rollup for all equipment model entities:
   a. Select **Configure** for the Risk roll-up configuration task.
   b. In the Security Exposure Management Workspace, follow the steps described in the Help Center for this section.
3. Configure the *Risk Rollup for VITs by Equipment Model Entity* scheduled job:
   a. Select **Configure** for the Daily Schedule job for risk roll up task.
   b. Security Exposure Management Workspace, follow the steps described in the Help Center for this section.

   Note: By default, the job is set to run daily. You can change this to fit your business needs by editing the **Run**, **Time zone**, and **Time** fields.

4. To avoid getting the wrong risk score and rating for remediation tasks, change the **Table** field in the **OT Devices with No sites Assigned Rollup** record:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **All** > **System Definition** > **Scripts - Background**.

b. In the **Run script** field, add the following script.

```
var gr = new GlideRecord('sn_vul_rollup');

gr.get('sys_id','24973dc4939e42900b1566f4548918eb');

gr.table = 'sn_ot_metric';

gr.update();
```

c. Select **Run script**.

d. To check the value of the **Table** field in the **OT Devices with No sites Assigned Rollup** record and run the scheduled job, navigate to **All** > **Vulnerability Response** > **Administration** > **Vulnerability Rollup Calculator**.

e. Select the **OT Devices with No sites Assigned Rollup** record.

f. Ensure that the **Table** field is set to **OT Metric [sn_ot_metric]**.

g. Run the scheduled job.

After running the job, the correct VIT risk scores and ratings are rolled up to the remediation tasks.

5. Configure the entities for risk score roll-up:

a. Select **Configure** for the Set All Entities for Risk score Roll-Up Job task.

b. Security Exposure Management Workspace, follow the steps described in the Help Center.

Install certified Vulnerability Response integrations

Integrate certified third-party applications that enhance functionality of OT vulnerability management.

Search the ServiceNow® Store for Operational Technology Certified integrations for the Operational Technology Vulnerability Response application, and install those applicable to your environment.

Operational Technology Vulnerability Response Integrations

The Operational Technology Vulnerability Response application includes support for third-party integrations.

The following third-party integrations are currently supported.

- Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)
- Vulnerability Response Integration with Claroty CTD.

Vulnerability Response Integration with Claroty CTD

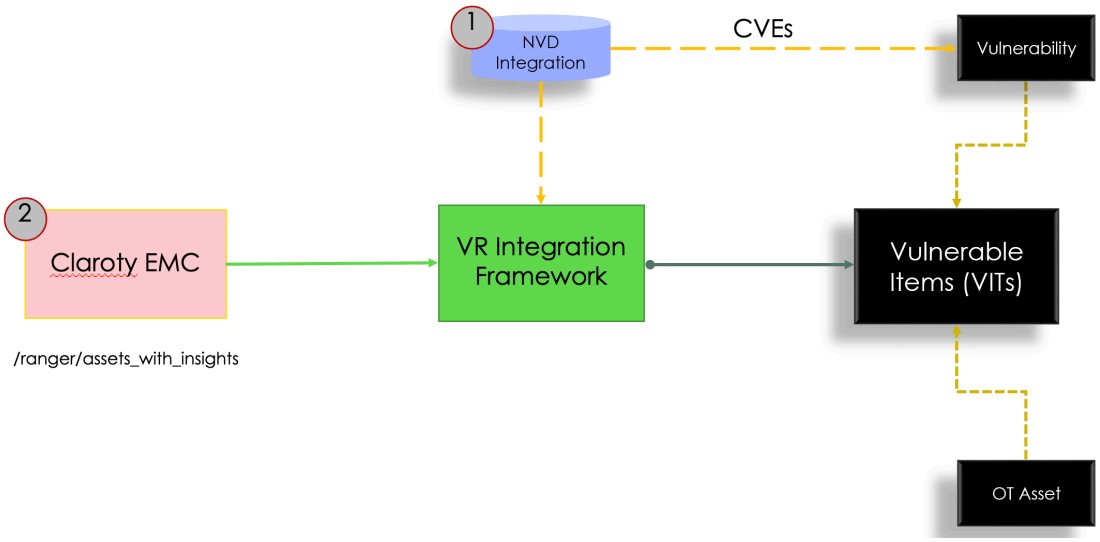
The Vulnerability Response Integration with Claroty Continuous Threat Detection (CTD) uses vulnerability data imported from Claroty CTD to enable risk-based action within the production process.

Use this Vulnerability Response Integration with the ServiceNow® Operational Technology Vulnerability Response application to track, prioritize, and resolve vulnerabilities used in the production process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following image shows the process for the Vulnerability Response Integration with Claroty CTD.

Process for the Vulnerability Response Integration with Claroty CTD



Before you run the Vulnerability Response Integration with Claroty CTD, you must run the National Vulnerability Database (NVD) integration. The NVD integration fetches published Common Vulnerabilities and Exposures (CVEs) from the NVD and populates them in ServiceNow. Then when you run the Vulnerability Response Integration with Claroty CTD application, the application identifies the vulnerabilities for each device and creates vulnerable items (VITs).

Each VIT has a relationship with an Operational Technology (OT) device, or Configuration Item (CI), and the vulnerability that's detected. The vulnerability integration framework establishes a connection with the Claroty Enterprise Management Console (EMC) and pulls the vulnerabilities for all OT devices.

Note: The Claroty CTD EMC platform insights API has a limitation of 10 CVEs. Therefore, only 10 CVEs are provided to ServiceNow by Claroty. However, the xDome platform doesn't have this limitation.

Key features

- Import common vulnerabilities and exposures (CVEs) associated with Operational Technology (OT) devices from Claroty CTD. Create vulnerable items (VITs) to provide a single view of OT device vulnerability data and how it affects the production process.
- Run imports of newly detected vulnerabilities automatically on your own schedule.
- Use assignment rules to route VITs automatically for remediation to local site-based teams that can take risk-based actions.

Install Vulnerability Response Integration with Claroty CTD

Install the Vulnerability Response Integration with Claroty CTD (sn_clarotyctdvr). The application includes installs related ServiceNow® Store applications and plugins if they aren't already installed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- Review the Vulnerability Response Integration with Claroty CTD application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.
- Vulnerability Response Integration with Claroty CTD requires the following ServiceNow Store applications. Ensure that these applications are installed before you install the Vulnerability Response Integration with Claroty CTD.

  CMDB CI Class Models store app

  This integration uses the Operational Technology extension classes that are part of the CMDB CI Class Models application. For more information, see CMDB CI Class Models app.

  Service Graph Connector Integration for Claroty CTD

  This integration uses the Operational Technology Manager application to automate the import of sites, detected devices by each site, connections (or base systems), and installed programs to the Configuration Management Database (CMDB). To install the Service Graph Connector Integration for Claroty CTD, see Install Vulnerability Response Integration with Claroty CTD.

Role required: admin

About this task

The following items are installed with Vulnerability Response Integration with Claroty CTD:

- Vulnerability response plugin
- Vulnerability Response Integration with NVD

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Vulnerability Response Integration with Claroty CTD application (sn_clarotyctdvr) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you can't find the application, you might have to request it from the ServiceNow Store.

   In the list next to the **Install** button, the versions that are available to you are displayed.
3. Select a version from the list and select **Install**.

   In the Review Installation Details dialog box, any dependencies installed with your application are listed.
4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. Select **Install**.

Assign Vulnerability Response Integration with Claroty CTD roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Vulnerability Response Integration with the Claroty CTD application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
When you're assigned the roles listed in the following table, you can use the Vulnerability Response Integration with Claroty CTD application.

Assign roles to admin users or user groups as needed.

For more information about the roles available for the Vulnerability Response Integration with Claroty CTD application, see Vulnerability Response Integration with Claroty CTD roles.

Procedure

Assign roles to users or groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Vulnerability Response Integration with Claroty CTD roles

Roles control access to features and capabilities in the Vulnerability Response Integration with Claroty CTD.

The following table describes the roles and permissions for the Vulnerability Response Integration with Claroty CTD.

Vulnerability Response Integration with Claroty CTD roles

Role	Description
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view OT VR integration records.
OT VR Integration Admin [sn_otvr.integration_admin]	Can configure and execute the OT VR integration.
MID server [mid_server]	Can configure a MID Server.

Required permissions in Claroty CTD

Review that the following user permissions have the **View** access enabled in Claroty CTD to collect data from Claroty CTD to ServiceNow:

- Visibility
- Investigation
- Threat Detection
- Risk and Vulnerabilities

Run the National Vulnerability Database integration

Run the National Vulnerability Database (NVD) integration to import data from the National Institute of Standards and Technology (NIST) NVD product. Running the NVD integration helps

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

you determine the severity and details of Common Vulnerabilities and Exposures (CVEs) found in your environment.

Before you begin

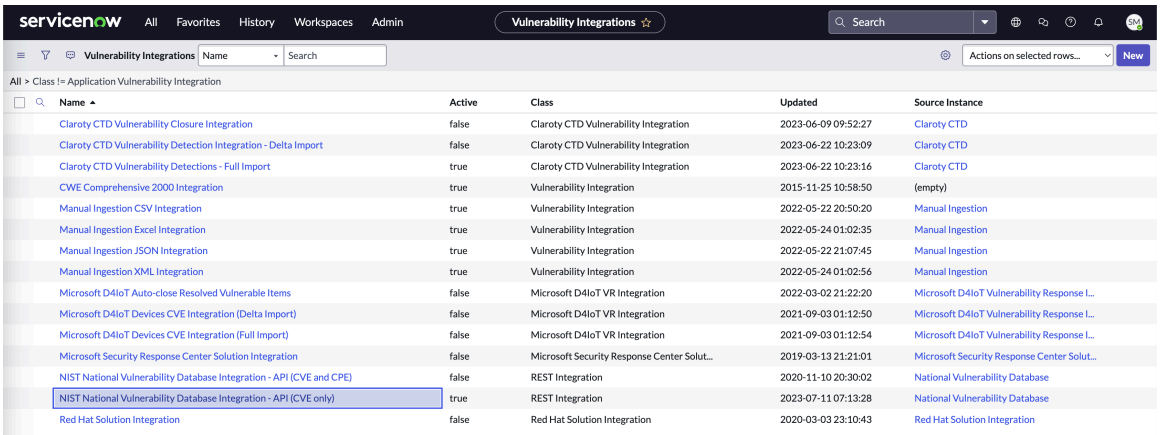
Before you run the NIST NVD integration on your instance, the installation and configuration steps must be completed. Completing the installation and configuration ensures that the NVD product properly integrates with the Operational Technology Vulnerability Response application.

To install the NVD plugin, see Install the Vulnerability Response Integration with the NIST National Vulnerability Database.

Role required: admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.
2. Select the NIST NVD integration - API (CVE only) record.



Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response I...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response I...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response I...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. In the **Import Since** field, set the value to **NULL**.
4. Select **Execute Now**.

Configure the Vulnerability Response Integration with Claroty CTD

Configure the Vulnerability Response Integration with Claroty CTD to begin importing data.

Use the Claroty CTD Vulnerability Integration Guided Setup to complete the configuration.

To access the Claroty CTD Vulnerability Integration Guided Setup, navigate to **Claroty CTD Vulnerability Integration** > **Admin** > **Setup**.

Connect to the Claroty CTD

Connect to the Claroty CTD to begin the Vulnerability Integration setup.

Before you begin

Before performing the setup, change the application scope to **Vulnerability Response Integration with Claroty CTD** by selecting the globe icon ( ) in the navigation bar.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Claroty CTD Vulnerability Integration** > **Admin** > **Setup**.
2. In the Connect to Claroty CTD section, select the **Setup Connections** task.
3. On the Setup Connections task page, select **Configure**.
   The Claroty CTD Connection Manager page opens.
4. On the form, fill in the following fields.

Connect to Claroty CTD form

Field	Description
Claroty EMC URL	URL of the Claroty CTD Enterprise Management Console (EMC).
Minimum CVSS Score	This field is visible if you select 5.0.x or 5.1.x as the CTD version. If applicable, you can filter which vulnerabilities are imported based on their Common Vulnerability Scoring System (CVSS) score. The filter is actually values that ranges from 0.0 to 10.0 and acts as a greater than or equal filter. For example, if you enter the score value as **9** the integration imports vulnerabilities with a CVSS score of 9.0-10.0.
EPSS Score (Optional)	This field is visible if you select 5.1.x or later as the CTD version. If applicable, you can filter which vulnerabilities are imported based on their Exploit Prediction Scoring System (EPSS) score. The EPSS Score uses the following values that acts as a filter: Critical, High, Medium, and Low. You can select only one option. For example, if you select **Critical** as the EPSS Score value, Claroty CTD only imports the vulnerabilities with a **Critical** EPSS score.
User Name	Claroty account user name.
Password	Claroty account password.
MID Server	If your Claroty EMC is on-premises, a MID Server may be required. If so, select a MID Server here.

5. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select **Test Connection**.
   If the connection test is successful, a `Results 200` output message appears. An unsuccessful connection attempt displays the error code and the message received from Claroty.

Activate the Delta Import integration

Activate the Delta Import integration to import vulnerabilities from Claroty CTD.

Before you begin

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see Run the National Vulnerability Database integration.

Role required: admin

About this task

The Delta Import integration imports vulnerabilities from Claroty CTD from the last successful integration run. By default, the first run imports the past 90 days of data. Clearing the **Start time** field results in a full import.

Procedure

1. Navigate to **All** > **Claroty CTD Vulnerability Integration** > **Admin** > **Setup**.
2. In the Configure Integration Scheduled Jobs section, select the **Activate Delta Import Integration** task.
3. Select **Configure**.
4. Ensure the Delta Import integration record is set to **Active**.
5. Ensure that the **Run** field is set to **On Demand**.
6. **Optional:** To execute a full import, clear the **Start time** field.
7. Select **Update**.

Run the Vulnerability Integration after the Service Graph Connector

Run the Claroty CTD Vulnerability Integration after running the Service Graph Connector for Claroty CTD. Running the Vulnerability Integration immediately after running the Service Graph Connector ensures that the most up to date CMDB information is populated from Claroty CTD.

Before you begin

The Service Graph Connector Integration for Claroty CTD must be configured and active in order to run the Vulnerability Response Integration to run after the Service Graph Connector.

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see Run the National Vulnerability Database integration.

Role required: admin

Procedure

1. Navigate to **All** > **Claroty CTD Vulnerability Integration** > **Admin** > **Setup**.
2. In the Configure Integration Scheduled Jobs task, select the **Run After Service Graph Connector** tab.
3. Select **Configure**.
4. For the Run After SGC - Claroty CTD Vulnerability Detection Integration - Delta Import record, activate it by selecting the **Active** option.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Ensure the **Run** field is set to **After Parent Runs**.
6. Ensure the **Parent** field is set to **SG-OT Claroty CTD Assets Scheduled Import**.
7. Select **Update**.

Activate the Auto-Closure Integration

Activate the auto-closure integration to close the corresponding ServiceNow Vulnerability Detections.

Before you begin

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see Run the National Vulnerability Database integration.

Role required: admin

About this task

There are two closure integration jobs available for the Vulnerability Response Integration with Claroty CTD:

- Claroty CTD Resolved Vulnerability Closure Integration
- Claroty CTD Full Vulnerability Closure Integration

The Claroty CTD Resolved Vulnerability Closure Integration checks for the vulnerable items (VITs) that have been marked as **Resolved** in the ServiceNow Configuration Management Database (CMDB). It then queries Claroty CTD for these VITs and closes them based on the response obtained from Claroty CTD.

The Claroty CTD Full Vulnerability Closure Integration checks for all VITs regardless of their state (Resolved or not) in the ServiceNow CMDB. It then queries Claroty CTD for all the VITs, and closes those that don't have a corresponding CVE entry in Claroty CTD.

Procedure

1. Navigate to **All** > **Claroty CTD Vulnerability Integration** > **Admin** > **Setup**.
2. In the Configure Integration Scheduled Jobs task, select the **Activate Auto-Closure Integration** tab.
3. Select **Configure**.

   Note: The auto-closure integration is pre-configured to run after the Delta Import, so no scheduling is required.

4. Ensure that the **Run** field is set to **On Demand**.
5. Ensure that the record is set to **Active**.
6. Select **Update**.

Configure the Full Import Integration from Claroty CTD

Configure the Full Import Integration to import the entire vulnerability inventory of a device from Claroty CTD.

Before you begin

Before scheduling the import of Claroty CTD records, run the NVD integration to fix any issues. For more information, see Run the National Vulnerability Database integration.

Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The Claroty CTD Vulnerability Detections - Full Import integration imports the entire vulnerability inventory of a device from Claroty CTD without respect to a certain date. This integration is useful if the daily delta imports haven't imported all the necessary vulnerability data.

Note: If you're using Claroty CTD v5.1, there's no limit on the number of Common Vulnerabilities and Exposures (CVEs) you can import per configuration item (CI). If you are using version 5.0.x or an earlier version of Claroty CTD, the number of CVEs you can import is limited to 10 per CI.

For more information on using Operational Technology Vulnerability Response Integration with Claroty CTD, see Connect to the Claroty CTD.

Procedure

1. Navigate to **All** > **Claroty CTD Vulnerability Integration** > **Admin** > **Setup**.
2. In the Configure Integration Scheduled Jobs task, select the **Configure Full Import Integration** tab.
3. Select **Configure**.
4. Ensure that the **Run** field is set to **On Demand**.
5. Ensure that the record is set to **Active**.
6. Select **Update**.

Set the system properties installed for the Vulnerability Response Integration with Claroty CTD

Set the system properties for the Vulnerability Response Integration with Claroty CTD so that you can enable the properties as needed.

Before you begin

Before performing the setup, change the application scope to **Vulnerability Response Integration with Claroty CTD** by selecting the Globe icon ( ) in the navigation bar.

Role required: sn_otvr.integration_admin

Procedure

1. Navigate to **All** > **Claroty CTD Vulnerability Integration** > **Admin** > **Properties**
2. Configure the following system property records according to your requirement for your organization:

System properties

Name	Description	Type	Default value
sn_clarotyctdvr.api_token_length_in_minutes	Length of time the Claroty CTD API token is valid. Default is 480 minutes (8 hours).	integer	480
sn_clarotyctdvr.api_token_object	An object that indicates access to the API.	string	{"customer_name":"","first_name":"Serv for API","id":1,"last_name":null,"mail":null,"p

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description	Type	Default value
sn_clarotyctdvr.auto_close_detections	Auto-close detections Vulnerability Detections from Claroty CTD.	true, false	false
sn_clarotyctdvr.auto_close_detections_after_days	Detections in Claroty CTD will be auto-closed after a designated number of days since Last Found.	integer	90
sn_clarotyctdvr.default_api_page_size	Number of records to pull per page from the Claroty CTD API.	integer	500
sn_clarotyctdvr.detection_integration_delta_time_buffer	When importing data from the Claroty CTD API, a buffer of a designated number of hours is added before the "start time." This ensures that no records are missed in the Delta import.	integer	4
sn_clarotyctdvr.integration_default_days	By default, the first run of the integration imports data from a past number of days.	integer	90
sn_clarotyctdvr.logging.application	Application logging level	choice	info
sn_clarotyctdvr.require_ci_match	Require incoming CI to match the CMDB to create Vulnerability Detections.	true, false	true

3. Select **Update** and save your changes.

Data mapping for the Vulnerability Response Integration with Claroty CTD

This section specifies how fields from the Claroty CTD API are mapped to fields in the ServiceNow tables.

Vulnerability detection data mapping

Claroty CTD field	ServiceNow field	Notes
	Source	Always set to **Claroty CTD**.
Identified_on	First Found	
Last_updated	Last Found	
Status	Status	A status of **0** means **Open**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Claroty CTD field	ServiceNow field	Notes
		A status of **2** means **Closed/ Fixed**.
Resource_id	Configuration item	The configuration item (CI) is set through a CI lookup rule that searches the sys_object_source table for the Resource ID. For example, 33.1.

Vulnerability entry data mapping

Vulnerability entries are only created if an existing Common Vulnerabilities and Exposures (CVE) record is not found in the National Vulnerability Database Entry [sn_vul_nvd_entry] table. If the Claroty CTD Integration must create a CVE, it maps the following source fields listed in the table.

Claroty CTD field	ServiceNow field	Notes
Cve_id	ID	Example: CVW-2017-17562
Title	Summary	The integration adds [Claroty] to the Summary so that the NVD CVEs, backfilled by Claroty, are visible. For example, the [Claroty] Authentication Bypass Vulnerability in SIPROTEC.
Cvss	V3_base_score	
Published	Date_published	
Modified	Last_modified	

Errors for the Vulnerability Response Integration with Claroty CTD

You may encounter errors that need troubleshooting while you're working with the Vulnerability Response Integration with Claroty CTD.

Vulnerability Detection Integration (Data Retrieval)

Error message	Possible cause
Can't run a Claroty CTD Integration without a user name and password combo.	No user name or password is present on the integration configuration.
Can't run integration without a REST message and REST method specified.	On the Claroty CTD Integration job record, the REST message or REST method fields aren't populated.
Can't run integration without Claroty CTD server URL specified.	No URL is present on the integration configuration.
Can't run integration without the detection API resource path specified.	On the integration configuration, the detection_api_resource_path parameter isn't populated. The default is `/ranger/assets_with_insights`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Error message	Possible cause
Invalid response code {response code} received from Claroty CTD.	The response from the Claroty API was invalid. For example, the message `Invalid response code 401` is received from Claroty CTD. This invalid response code means **Unauthorized** and that the credentials (user name/password) are likely invalid.
Unable to read the count_total property from JSON data.	The count_total used for pagination wasn't present in the API response. It likely means that an invalid payload was received from Claroty CTD. Ensure that the Claroty CTD instance is reachable through the MID Server and examine the Data Source attachment `response.json` file to ensure that count_total exists.

Vulnerability Detection Integration (Data Processing)

Error message	Possible cause
Error writing attachment.	The system couldn't attach the response data to the Data Source. Contact your administrator for further assistance. A common cause for this error is that the MID Server user is missing the sn_vul.vr_import_admin role.
Attachment content is null: attachment sys_id = {sys_id}.	The Data Source attachment content is null. This could indicate an issue with the Claroty API itself, or an issue in ServiceNow. Contact your administrator for further assistance.
Couldn't find attachment with sys_id {sys_id}.	Data Source attachment wasn't found. Follow the same procedures for the preceding error.

Vulnerability Auto-Closure Integration (Data Retrieval)

Error message	Possible cause
Can't run a Claroty CTD Integration without a user name and password combo.	No user name or password is present on the integration configuration.
Can't run integration without a REST message and REST method specified.	On the Claroty CTD Integration job record, the REST message or REST method fields aren't populated.
Can't run integration without Claroty CTD server URL specified.	No URL is present on the integration configuration.
Can't run integration without the detection API resource path specified.	On the integration configuration, the detection_api_resource_path parameter

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Error message	Possible cause
	isn't populated. The default is `/ranger/assets_with_insights`.
Invalid response code {response code} received from Claroty CTD.	The response from the Claroty API was invalid. For example, the message `Invalid response code 401` is received from Claroty CTD. This invalid response code means **Unauthorized** and that the credentials (user name/password) are likely invalid.
Unable to read the count_total property from JSON data.	The count_total used for pagination wasn't present in the API response. It likely means that an invalid payload was received from Claroty CTD. Ensure that the Claroty CTD instance is reachable through the MID Server and examine the Data Source attachment `response.json` file to ensure that count_total exists.
Error parsing 'objects' array from response body.	Likely means that an invalid payload was received from Claroty CTD. Ensure that the Claroty CTD instance is reachable and check Outbound HTTP Logs to see if there was a valid response.

Vulnerability Auto-Closure Integration (Data Processing)

Error message	Possible cause
Failed to parse the Data Dictionary JSON.	The payload from the Data Source attachment was invalid JSON. Likely another error occurs before this error occurs. Ensure that the Claroty CTD instance is reachable and check Outbound HTTP Logs to see if there was a valid response.

Vulnerability Response Integration with Microsoft Defender for IoT (Azure)

The Vulnerability Response Integration with Microsoft Defender for IoT (Azure) uses data imported from Microsoft Defender for IoT (Azure) to enable risk-based action with the production process context.

Use the Vulnerability Response integration with the ServiceNow® Operational Technology Vulnerability Response application to track, prioritize, and resolve vulnerabilities on devices used in the production process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Key Features

- Import CVEs associated with OT devices from Microsoft Defender for IoT (Azure) and create vulnerable items (VITs) to provide a single view of OT devices vulnerability data with production process context.
- Run imports of vulnerabilities automatically on your own schedule.
- Using assignment rules, VITs can be automatically routed for remediation to local site-based teams to take risk-based action.

Install the Vulnerability Response for Microsoft Defender for IoT (Azure)

You can install the Vulnerability Response for Microsoft Defender for IoT (Azure) if you have the admin role. The application includes installs related ServiceNow® Store applications and plugins if they are not already installed.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- Review the Vulnerability Response for Microsoft Defender for IoT (Azure) application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.
- Vulnerability Response for Microsoft Defender for IoT (Azure) requires the following ServiceNow Store applications. Ensure that these applications are installed before you install the Vulnerability Response integration with Microsoft Defender for IoT.

  CMDB CI Class Models store app

  This integration uses the Operational Technology extension classes that are part of the CMDB CI Class Models application. For more information, see CMDB CI Class Models app.

  Service Graph Connector Microsoft Defender for IoT (Azure)

  This integration uses the Operational Technology Manager application to automate the import of sensor appliances, OT devices, and network connections. To install the Service Graph, see Service Graph Connector for Microsoft Defender for IoT (Azure).

Role required: admin

About this task

The following items are installed with Vulnerability Response for Microsoft Defender for IoT (Azure):

- Vulnerability Response plugin
- Vulnerability Response Integration with NVD

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Vulnerability Response Integration for Microsoft Defender for IoT (Azure) using the filter criteria and search bar.

   You can search for the application by its name or application scope ID. If you can't find the application, you may have to sync applications or request it from the ServiceNow Store and entitle your instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the list next to the **Install** button, the versions that are available to you are displayed.

3. Select a version from the list and select **Install**.

   In the Review Installation Details dialog box, any dependencies installed with your application are listed.

4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. Select **Install**.

Navigate to Guided Setup for the Vulnerability Response Integration with Microsoft Defender for IoT (Azure)

After installing the Vulnerability Response Integration with Microsoft Defender for IoT (Azure), navigate to the Guided Setup to walk you through the application's configuration.

Before you begin

Change the application scope to Vulnerability Response Integration with Microsoft Defender for IoT (Azure) by selecting the globe icon () in the navigation bar.

Role required: admin

Procedure

1. Navigate to **All** > **Azure D4IoT Vulnerability Integration** > **Admin** > **Guided Setup**.
2. Select **Get Started**.

Connect to the Microsoft Defender for IoT (Azure)

Connect to Microsoft Defender for IoT (Azure) to begin the Vulnerability Integration setup.

Before you begin

Review that you have **Security Reader** permission enabled on Microsoft Defender for IoT Azure, which provides the following user actions:

- Download sensor endpoint details
- View values on the Sites and sensors page
- View Azure device inventory
- View Azure workbooks
- View Defender for IoT settings
- Download OT threat intelligence packages

For more information, see Azure user roles and permissions for Defender for IoT.

Role required: admin

Procedure

1. Navigate to **All** > **Azure D4IoT Vulnerability Integration** > **Admin** > **Guided Setup**.
2. In the Connect to Microsoft Defender for IoT (Azure) section, select the **Setup Connections** task.
3. On the Setup Connections task page, select **Configure**.
   The Connect to Microsoft Azure Defender for IoT page opens.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. On the form, fill in the following fields.

Connect to Microsoft Azure Defender for IoT form

Field	Description
OAuth Token URL	The OAuth 2.0 token URL for login.microsoftonline.com. For example, `https://login.microsoftonline.com/<your tenant id>/oauth2/v2.0/token`.
OAuth Client ID	Your client ID.
OAuth Client Secret	Your client secret.
Page Size Limit	The maximum number of records to pull for each page of data. The default is 500.
Minimum CVSS Score	Only vulnerabilities with a CVSS score greater than or equal to this value are imported. The default is 0.0 for all vulnerabilities.
Run After Service Graph Connector Import	This is a recommended field that runs the vulnerability import immediately after the Service Graph Connector for Microsoft Defender for IoT (Azure) devices import is completed. This ensures the best probability of matching incoming vulnerability data to the CMDB. Most commonly, the value is `SG-OT Microsoft Azure D4IoT Devices Scheduled Import`. When selecting this field, leave the **Azure D4IoT Vulnerability Detection Integration - Full Import** scheduled job set to run **On Demand**. This ensures that the Service Graph Connector device import can execute it as a child job once the devices import is complete.
Daily Import Time	If you're not using the **Run After Service Graph Connector Import** field, you can set the daily import time of the integration using this field. **Note:** If you have a scheduled import selected for the **Run After Service Graph Connector Import** field, this field is unavailable.

5. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select **Test Connection**.
   If the connection test is successful, a `Results 200` output message appears. An unsuccessful connection attempt displays the error code and the message received from Microsoft Defender for IoT (Azure).

Run the National Vulnerability Database integration

Run the National Vulnerability Database (NVD) integration to import data from the National Institute of Standards and Technology (NIST) NVD product. Running the NVD integration gives you the foundational Common Vulnerabilities and Exposures (CVEs) data referenced by the Microsoft Defender for IoT (Azure) vulnerabilities to help you determine the severity and details of vulnerabilities in your environment.

Before you begin

Before you run the NIST NVD integration on your instance, the installation and configuration steps for the integration must be completed. Completing the installation and configuration ensures that the NVD product properly integrates with the Operational Technology Vulnerability Response application.

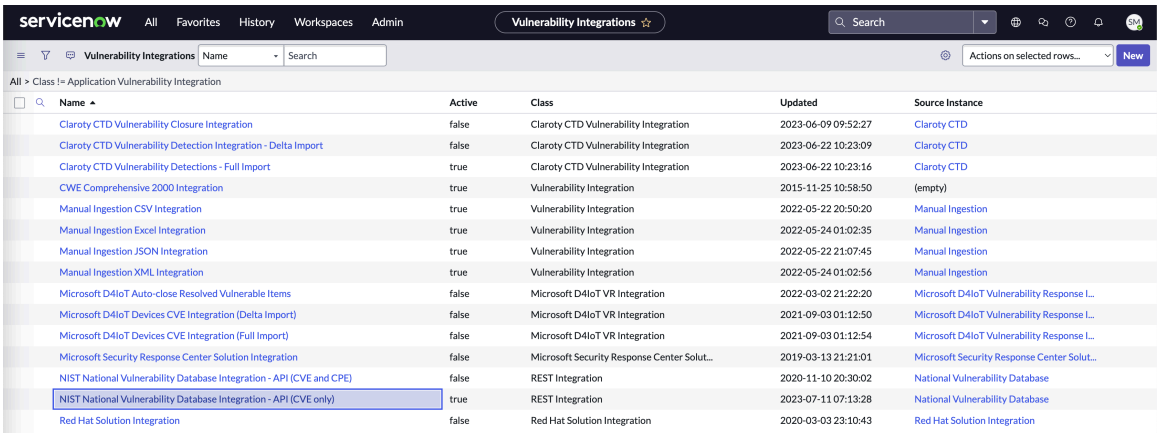
To install the NVD plugin, see Install the Vulnerability Response Integration with the NIST National Vulnerability Database.

Role required: admin

Procedure

1. Navigate to **All** > **Azure D4IoT Vulnerability Integration** > **Admin** > **Guided Setup**.
2. In the **Configure Integration** section, select **Configure** next to the **Import National Vulnerability Database (NVD) CVE Entries** task.
3. Depending on which is active, select either the NIST NVD integration - API (CVE only) record or the NIST National Vulnerability Database Integration – API (CVE and CPE) record.

   Note: The NIST NVD integration - API (CVE only) record is most commonly active by default.



Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response I...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response I...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response I...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

4. To edit the record, set the **Application scope** to **Vulnerability Response Integration with NVD** using the globe (🌐) icon.
5. In the **Import Since** field under the **Integration Details** tab, set the value to a date in the past.

   Note: This is required so a full import of the NVD occurs. The recommended date is `1999-01-01 00:00:00`.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select **Save**.
7. Select **Execute Now**.

Configure integration scheduled jobs

Activate the scheduled jobs that import vulnerability data.

Before you begin

Before scheduling the import of Microsoft Defender for IoT (Azure) records, run the NVD integration to fix any issues. For more information, see Run the National Vulnerability Database integration.

Role required: admin

Procedure

1. Navigate to **All** > **Azure D4IoT Vulnerability Integration** > **Admin** > **Guided Setup**.
2. In the **Configure Integration** section, select **Configure** next to the **Verify and Activate Integration Scheduled Jobs** task.
3. Select the **Azure D4IoT Vulnerability Detection Integration - Full Import** job.
   This job imports vulnerability detections from Microsoft Defender for IoT (Azure).
4. Next to the **Active** field, select the check box.
   You can also adjust the schedule if additional changes are needed. If you configured the vulnerability integration to **Run After Service Graph Connector Import** in the **Setup Connections** task, you should leave this job set to run **On Demand**. For more information about the **Setup Connections** task, see Connect to the Microsoft Defender for IoT (Azure).
5. Select **Update**.
6. Select the **Azure D4IoT Vulnerability Closure Integration** job.
   Azure D4IoT Vulnerability Closure Integration is a detection job that determines which detections have been deleted from Microsoft Defender for IoT (Azure) and then closes them in ServiceNow.
7. Next to the **Active** field, select the check box.
   It's recommended to keep the **Run** field as **On Demand**.
8. Select **Update**.

Activate Auto-Close Stale Detections

Configure the system properties that are used in the auto-close stale detections process to automatically close vulnerabilities that are no longer in your environment.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Azure D4IoT Vulnerability Integration** > **Admin** > **Guided Setup**.
2. In the **Auto-Close Stale Detections (Optional)** section, select the **Activate Auto-Close Stale Detections** task.
3. Select **Configure**.
4. In the **Azure D4IoT VR Auto Close Properties** page in the **Auto-close stale detections from Microsoft Azure Defender for IoT?** field, select **Yes**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. In the **Detections from Microsoft Azure Defender for IoT will be auto-closed after (value) days since they were updated** field, enter the number of days to wait until the detections automatically close.
   The default is 90.
6. Select **Save**.

Activate the Auto-Close Stale Detections job

Activate the scheduled job to auto-close stale detections on a recurring basis.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **Azure D4IoT Vulnerability Integration** > **Admin** > **Guided Setup**.
2. In the **Auto-Close Stale Detections (Optional)** section, select the **Activate Auto-Close Stale Detections Scheduled Job** task.
3. Select **Configure**.
4. Next to the **Active** field, select the checkbox.
5. **Optional:** In the **Run** field, select the option that fits your needs.
   By default, the field is set to **On Demand** but you can change it based on your needs. For example, you can select **Daily** and choose the hour and minute of the day in the **Time** field that appears.
6. Select **Save**.

Support for the Vulnerability Response Integration with Microsoft Defender for IoT (Azure)

You can refer to this section for questions regarding data mapping and error handling.

Data mapping

The following tables describe the data mapping fields used for vulnerability detection and National Vulnerability Database (NVD) entries in the Microsoft Defender for IoT (Azure) application and if there's an equivalent entry used after the data is imported into the ServiceNow CMDB.

Vulnerability Detection

Microsoft Defender for IoT (Azure) field	ServiceNow field
N/A	source **Note:** Always set this field to **Microsoft Azure Defender for IoT**.
name	detection_key
N/A	status **Note:** This field is set to **0**, meaning open, by default.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

NVD entries

Microsoft Defender for IoT (Azure) field	ServiceNow field
properties/vulnerabilityid	id
	source **Note:** This field is set to **NVD** by default.
properties/description	summary
properties/score	score
properties/exploittype	Exploit exists If the API data indicates an exploit exists, the integration sets this field to **Yes**.
properties/exploittype	public_exploit If the API data indicates an exploit exists, the integration sets this field to **Yes**.

Configuration item (CI) lookup

The CI Lookup is performed using the **deviceid** from Microsoft Defender for IoT (Azure). The sys_object_source table, populated by the Service Graph Connector, is searches for the the matching deviceid. If a match is found, the detection and vulnerable item are linked to that CI.

Note: By default, a CI match is required to insert vulnerability detections. This helps minimize unclassed hardware CIs in your CMDB. To change this behavior, you can set the **sn_msftd4iotazvr.require_ci_matchsystem** property to **false**. Setting the property to false allows the creation of unclassed hardware CIs if a CI match isn't found.

Error handling

The integration is designed to be mostly pre-configured, so you only need to enter your Azure Tenant ID, Client ID, and Client Secret. Log messages from the application are viewable in the System Logs from the **sn_msftd4iotazvr** source. Additional relevant log message can also appear from the **sn_vul** source.

If the integration run fails, the error is shown in the **Notes** field on the integration run. The state is set to **Complete** with a substate of **Failed**.

The Import Queue (sn_vul_ds_import_q_entry) table contains all the pending transformation requests. You can filter this table to only show items that have a **status** of **Processing** to view what is currently under transformation.

The following tables describes the error messages and possible causes during data retrieval and data processing.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Detection Integration (Data Retrieval)

Error message	Possible cause
Cannot run integration without a REST message and REST method specified	On the Detection Integration job record, the **REST message** or **REST method** fields are not populated.
Cannot run integration without Microsoft Defender for IoT (Azure) oauth_client_id specified	On the Integration Instance, the **OAuth Client ID** is not populated.
Cannot run integration without Microsoft Defender for IoT (Azure) oauth_client_secret specified	On the Integration Instance, the **OAuth Client Secret** is not populated.
Cannot run integration without the detection API resource path specified	On the Integration Instance, the detection API resource path is not populated. The default is `https://management.azure.com/providers/Microsoft.ResourceGraph/resources`
Cannot run integration with API version specified	On the Integration Instance, the API version is not populated. The default is 2021-03-01.
Invalid response code {response code} received from Microsoft Defender for IoT (Azure)	The response from the Microsoft API is invalid. For example, the invalid response code 401 received from Microsoft Defender for IoT (Azure) means **Unauthorized**. The credentials or OAuth Token are likely invalid.
Failed to parse the JSON response body	The JSON response received is invalid if it isn't able to be parsed. This means that no data was received. Ensure that the credentials are correct and no other errors occur.
Error writing attachment	The system couldn't attach the response data to the data source. You likely need to contact your system administrator for further troubleshooting. A common cause for this error is that the MID Server or **Run as** user is missing the sn_vul.vr_import_admin role.
Attachment content is null: attachment sys_id = {sys_id}	The Data Source attachment content is null. This could indicate an issue with the Microsoft API itself, or an issue in ServiceNow. Contact your system administrator for further troubleshooting.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Detection Integration (Data Retrieval) (continued)

Error message	Possible cause
Could not find attachment with sys_id {sys_id}	Data source attachment was not found. This could indicate an issue with the Microsoft API itself, or an issue in ServiceNow. Contact your system administrator for further troubleshooting.

Vulnerability Detection Integration (Data Processing)

Error message	Possible cause
Cannot create a Detection without a vulnerability ID	A vulnerability ID was not present for the record. This is most likely caused by an issue with the Microsoft API.

Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)

The Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) uses data imported from Microsoft Defender for IoT (On-premises Management Console) to enable risk-based action with the production process context.

Use the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application to track, prioritize, and resolve vulnerabilities on devices used in the production process.

Key Features

- Import CVEs associated with OT devices from Microsoft Defender for IoT (On-Premises Management Console) and create vulnerable items (VITs) to provide a single view of OT devices vulnerability data with production process context.
- Run imports of newly detected vulnerabilities automatically on your own schedule.
- Using assignment rules for VITs can be automatically routed for remediation to local site-based teams to take risk-based action.

Install the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)

You can install the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) if you have the admin role. The application includes installs related ServiceNow® Store applications and plugins if they are not already installed.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- Review the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application listing in the ServiceNow Store for information on dependencies, licensing or subscription requirements, and release compatibility.
- Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) requires the following ServiceNow Store applications. Ensure that these applications are

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

installed before you install the Vulnerability Response integration with Microsoft Defender for IoT.

CMDB CI Class Models store app

This integration uses the Operational Technology extension classes that are part of the CMDB CI Class Models application. For more information, see CMDB CI Class Models app.

Service Graph Connector Microsoft Defender for IoT (on-premises)

This integration uses the Operational Technology Manager application to automate the import of sensor appliances, OT devices, and network connections. To install the Service Graph, see Service Graph Connector for Microsoft Defender for IoT (On-premises Management Console).

Role required: admin

About this task

The following items are installed with Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console):

- Vulnerability response plugin
- Vulnerability Response Integration with NVD

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find the application, you might have to request it from the ServiceNow Store.

   In the list next to the **Install** button, the versions that are available to you are displayed.
3. Select a version from the list and select **Install**.

   In the Review Installation Details dialog box, any dependencies installed with your application are listed.
4. If you're prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. Select **Install**.

Assign Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application.

Before you begin

Role required: admin

About this task

Users with the roles that are listed in the following tables can use the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application.

Assign roles to admin users or user groups as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) roles

Role	Description
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view OT VR integration records.
OT VR Integration Admin [sn_otvr.integration_admin]	Can configure and execute OT VR integration.
MID server [mid_server]	Can configure MID Server.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Run the National Vulnerability Database integration

Run the National Vulnerability Database (NVD) integration to import data from the National Institute of Standards and Technology (NIST) NVD product. Running the NVD integration helps you determine the severity and details of Common Vulnerabilities and Exposures (CVEs) found in your environment.

Before you begin

Before you run the NIST NVD integration on your instance, the installation and configuration steps must be completed. Completing the installation and configuration ensures that the NVD product properly integrates with the Operational Technology Vulnerability Response application.

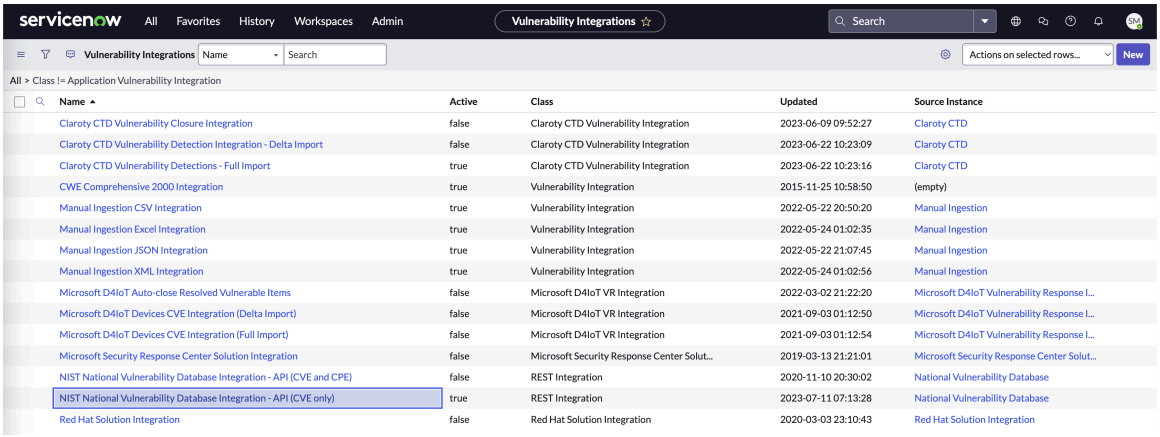
To install the NVD plugin, see Install the Vulnerability Response Integration with the NIST National Vulnerability Database.

Role required: admin

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**.
2. Select the NIST NVD integration - API (CVE only) record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



3. In the **Import Since** field, set the value to **NULL**.
4. Select **Execute Now**.

Configure the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console)

Configure the record for the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) integration.

Before you begin

Use the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) guided setup to complete the configuration. To access the Guided Setup, navigate to **MSFT D4IoT Vulnerability Integration** > **Administration** > **Guided Setup**.

Role required: sn_otvr.integration_admin and mid_server

Procedure

1. Navigate to **All** > **MSFT D4IoT Vulnerability Integration** > **Administration** > **Configurations**.
2. Click **New**.
3. On the form, fill in the fields.
   For a description of the field values, see Microsoft Defender for IoT VR Configuration form.
4. Click **Save and Verify Credentials**.

Microsoft Defender for IoT VR Configuration form

Use the Microsoft Defender for IoT VR Configuration form to configure the Vulnerability Response for Microsoft Defender for IoT (On-premises Management Console) application.

Microsoft Defender for IoT VR Configuration form

Field	Description
Name	The name of the configuration.
Integration instance	The instance for the configuration. The available default integration instance is the Microsoft Defender for IoT Vulnerability Response instance.
Endpoint URL	The URL of the Microsoft Defender for IoT Management Console.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Microsoft Defender for IoT VR Configuration form (continued)

Field	Description
	For example: `https://10.10.0.222/external/v3/integration/devicecves`
MID server	The MID Server used for the integration.
API key	The token needed to access the Central Manager APIs. For information about creating an API key in the Microsoft Defender for IoT management console, see https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis.
Page size	The number of devices per page in the Microsoft API response. The default page size is 50.
CVSS V2 Score	The vulnerabilities with the score greater than or equal to the configured CVSS V2 score is considered for the import of CVEs and creation of Vulnerable Item (VIT) records. The default value is set to 0.
Auto-close Resolved VIs	If the VIT record is set to resolved, it can be closed automatically if the CVE no longer appears in the API response from Microsoft Defender for IoT for that OT device.
Wait days to reopen a Resolved VI	When a VIT is resolved, it can take a while for Microsoft Defender for IoT to confirm if the vulnerability is resolved based on the OT device's communication in the network. Define the number of days to wait before reopening the resolved VIT when the NIDS cannot confirm it as Closed.

Configure import schedules

Configure the import schedules to access the Microsoft Defender for IoT records.

Before you begin

Before scheduling the import of Microsoft Defender for IoT records, run the NVD integration to fix any issue. For more information, see Run the National Vulnerability Database integration.

Role required: admin

Procedure

1. Navigate to **All** > **MSFT D4IoT Vulnerability Integration** > **Administration** > **Integrations**.
2. From the list of records, select your record:
   - The **Full Import** schedule imports all the vulnerabilities for all OT devices.

     Note: Frequent execution of the Full Import Schedule is not recommended because the number of records can be high.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The **Delta Import** schedule can be configured by default to run after the Microsoft Service Graph Connections integration. See Configure the system ID of the OT Vulnerability Response integration.
- Use the **Auto-close Resolved VIT Import** schedule if the vulnerability on the OT device is resolved. The Vulnerable Items (VITs) are closed automatically based on the confirmation from the scanner.

If the scope is not in the correct application, the message `To edit this record click here` appears on the top of the page.

3. Click **here** to edit the record.
4. Select the **Active** check box to change **Active** to **true**.
5. Select **Schedule** from the drop-down list as required.
6. Click **Execute Now**.

Configure the system ID of the OT Vulnerability Response integration

Configure the system ID to import integration records fully after the Microsoft SGC Connections integration.

Before you begin
Role required: admin

About this task
This configuration is strongly recommended to ensure all OT devices are in the CMDB that may have vulnerabilities reported against them.

Procedure
1. Navigate to **All** > **Service Graph Connector Microsoft D4 IoT** > **Properties**.

   If the scope is set to the wrong application, the message `To edit this record click here` appears at the top of the page.

2. Click **here** to edit the record.
3. Configure the system property `sn_msftd4iotsgc.ot.vr.integration.id` with the sys_id of the OT VR Integration.
4. Click **Save**.

Configure Auto-Close Stale Detections

Enable Auto-Close Stale Detections to automatically close stale vulnerable detections not recently found by your third-party integrations.

Before you begin
Role required: admin

About this task
The stale detections most likely result from a remediation targeted for a critical risk vulnerable item (VIT) that also addresses multiple additional lower criticality VITs with an **Open** state. Moving these VITs to **Closed** reduces the number of active VITs and vulnerability groups in your ServiceNow AI Platform instance.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Vulnerability Response** > **Administration** > **Auto-Close Configuration** > **Stale Detections**.

   The Auto-Close Stale Configuration form is displayed.

2. Fill in the fields.
3. For the **Auto-close stale detections based on** field, select **Detections last found** in the list. This option searches for the most current, or latest date that detections were found again by the scanner.

   Note: The **Devices last scanned** option is not applicable for OT scanners.

   Starting from v22.0 of Vulnerability Response, you can configure additional options for your search. See Create auto-close rules for more information.

4. To enable the module, select the **Active** check box.
5. In the **Detections last found (days ago)** field, enter the age of older, stale detections in the number of days.

   The default is 90 days. You can enter any positive value for the number of days. This value is used to match a last detected date provided by Microsoft Defender for IoT. With 90 and **Detections last found** displayed, any vulnerable items not detected in the last 90 days are automatically closed.

6. **Optional:** To ignore stale detections that are mapped to deferred VITs or VITs currently in review for deferral, select the **Ignore the stale detections for deferred VIs** check box. If you leave this option disabled, any detections that match your criteria will be closed that mapped to deferred VITs, or to VITs that are in review for deferral. The deferred VITs, or VITs that are in review that correspond to these detections are also automatically closed based on the rollup logic. For more information on roll up logic, see Closing stale detections in Vulnerability Response.

   If you enable this option, any detections that match your criteria that map to deferred VITs, or to VITs that are in review for deferral, are skipped during auto-close.

7. **Optional:** Deselect the **Ignore stale detections for closed VIs** check box. By default, this check box is selected so that the closed VIT is not reopened when a new detection to this closed VIT is identified. For more information on roll up logic, see Closing stale detections in Vulnerability Response.
8. Select **Update**.

   The *Auto-Close Stale Detections* scheduled job runs daily. The job determines whether you have selected the date when detections were last found or the date when assets were last scanned. It then transitions the corresponding detections to the Stale state. It's important to note that the Auto-Close Stale Detection feature only closes stale detections for active integration instances. Vulnerable items and detections associated with active integration instances are closed. Starting from v21.1 of Vulnerability Response the scheduled job has been modified to take into account the common table [sn_vul_cmn_auto_close_rule].

   After the detections are marked as Stale, if the scanner reports finding that detection again, the Status field of the detections transitions to Open. The detection's corresponding vulnerable items are also reopened.

   Additionally, if the detection is marked as Stale, and the scanner finds that it is Fixed, the detection transitions to Closed. The state also rolls up to the VITs.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using Operational Technology Vulnerability Response

After you complete all required set up tasks, including importing vulnerable items from a third-party integration, you can use the Operational Technology Vulnerability Response application from the Industrial Workspace.

Industrial Workspace

To use Operational Technology Vulnerability Response, access the following landing page and menus from the Industrial Workspace.

For more information on the Industrial Workspace, see Industrial Workspace.

OTVR (PA) dashboard in the Industrial Workspace

Use the OTVR (PA) dashboard to track the volume, performance, and progress of your vulnerable items from the initial analysis and detection to the containment, or remediation. You can filter the reports by the assignment group, exploits, risk rating, or state to get insight into your vulnerability exposure and the services that are affected.

For more information about the OTVR (PA) dashboard, see Operational Technology Vulnerability Response (PA) dashboard

OT Vulnerability Risk Rollup dashboard overview

The Operational Technology (OT) Vulnerability Risk Rollup dashboard contains two tables for your vulnerability risk scores.

- Vulnerability risk table for your equipment model entities
- Vulnerability risk table for OT devices with no site assigned

List menu

Use the List menu to view all OT Vulnerable Item records that you have access to and remediation tasks that have either been assigned to you or to an assignment group that you are a member of.

- OT Remediation Tasks
  - Assigned to me
  - Assigned to my groups
- OT Vulnerable Items
  - Assigned to me
  - Assigned to my groups
  - My Exception Requests
  - All Exceptions

> **Note:** The All Exceptions list also shows exceptions with a **Rejected** state.

Navigate to records under the OT Remediation Tasks or OT Vulnerable Items list menus to get more OT-related context. To view the history of the record, you can view the **Activity** window in the record where various work notes, comments, and record updates are captured. You can also add new comments or work notes in the **Compose** window.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about remediation tasks, see Create a remediation task.

For more information on how to use the List view in the Industrial Workspace for Operational Technology Vulnerability Response, see Use the List view in the IT Remediation Workspace.

Equipment model menu

Use the Equipment Model Manager to view OT vulnerable items, and view and create remediation tasks associated with OT devices that are mapped to an equipment model entity.

Hardware Vulnerability Assessment

Use the Hardware Vulnerability Assessment menu to view and manage the vulnerabilities assessments that have performed on the firmwares of the OT devices in the inventory.

Use the following tabs in the Hardware Vulnerability Assessment menu to view all the assessments records and the vulnerable items that are created automatically:

- Fully matched assessments
- Partially matched assessments
- Vulnerable items
- Ignored assessments
- Awaiting Normalization

Related topics

Vulnerability Response Workspaces

View vulnerable items and solutions in the Industrial Workspace

View Operational Technology (OT) vulnerable items (VITs) and their respective preferred solutions or all available solutions provided by OT Vulnerability Solution Management in the Industrial Workspace.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace** > **List view ( )** > **OT Vulnerable Items** > **All** to view all OT VITS.
2. Navigate to the list of VITS.
   - Navigate to **All** > **Industrial Workspace** > **List view ( )** > **OT Vulnerable Items**.
   - Navigate to **All** > **Industrial Workspace** > **Equipment Model view ( )** > **Vulnerable Items**.

   a. Select a VIT from the displayed list.

   b. You can view the preferred solution or all the available solutions for the VIT, in the Remediation section of the VIT.

   c. If there's more than one solution available for the VIT, select Search in the **Preferred Solution** field to search and view all the available solutions for the VIT.
3. Navigate to **All** > **Industrial Workspace** > **List view ( )** > **Solutions**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. View the complete list of available vulnerability solutions by selecting the **All** list.

b. View the list of vulnerability solutions for their respective vulnerable items by selecting the **With vulnerable items** list.

Related topics

Operational Technology Vulnerability Solution Management

View vulnerability exceptions in the Industrial Workspace

You can use request an Operational Technology (OT) Admin to ignore a vulnerable item (VIT) as an exception.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace** > **List view (** **)** > **OT Vulnerable Items**.
   - View the VITs you have requested to be considered as exceptions by selecting **My Exception Requests** list.
   - View the VIT exceptions requested by all the users in your OT environment by selecting **All Exception Requests** list.
   - View all the approved VIT exceptions in your OT environment by selecting **All Exceptions** list.
2. Navigate to **All** > **Industrial Workspace** > **List menu (** **)** > **OT Vulnerability Exception Approvals**.

   View all the VIT exceptions requests assigned to you for approval or already approved by you by selecting **Assigned to me** list.

   Use this menu to view any change of State for approvals and details of requested approvals for a specific Exception that has been triggered from the Industrial workspace.

Create a remediation task

Create remediation tasks associated with OT devices that are mapped to an equipment model entity.

Before you begin

Role required:sn_otvr.remediation_owner

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the **Equipment model** page.
3. In the **Equipment model view for** field, select the site that you want to view the equipment model information for.
4. Select the appropriate equipment model entity and navigate to the **Vulnerable Items** related list tab.
5. Select the vulnerable item records you want to add to the remediation task, then select **Create remediation task**.
6. Provide all the required details for the remediation task.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Assignment group field automatically assigns based on the site assignment group.

7. Select **Save** to create the task record.

Result

Once you create a remediation task, the task is picked up during the next scheduled maintenance determined by your equipment model entity maintenance schedule. For more information about equipment model entity schedules, see Managing equipment models.

You can also manually select a start time for a remediation task. For more information about selecting a start time, see Select a start time for a remediation task.

Select a start time for a remediation task

Select an expected start time for an Operational Technology (OT) remediation task by using the time slots in the equipment model entity schedules.

Before you begin

Role required: sn_otvr.remediation_owner

About this task

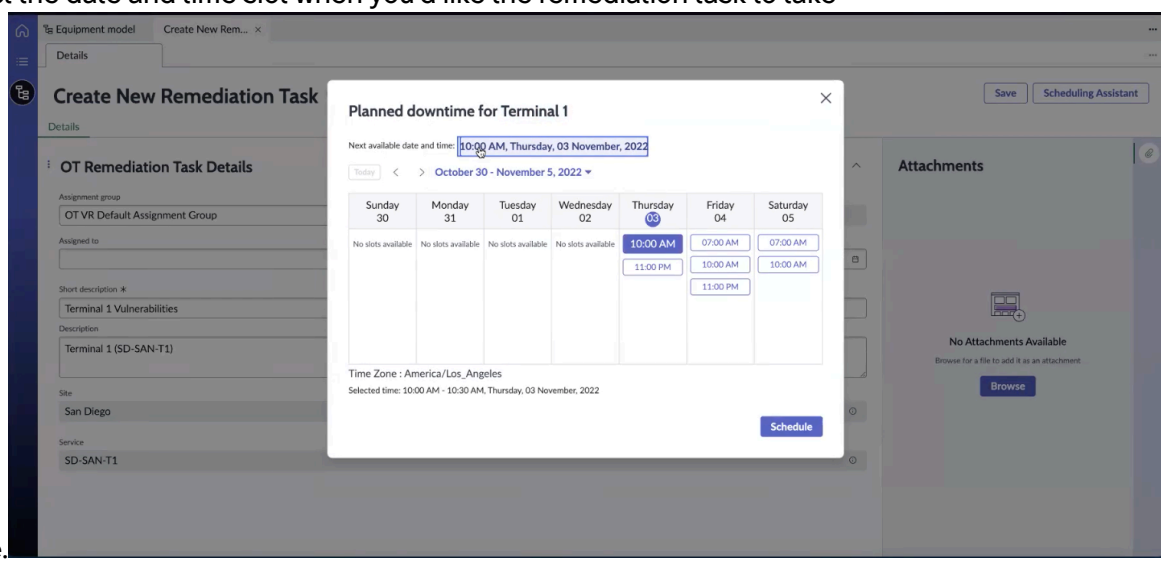
There are two ways to manually select a start time for an OT remediation task.

- You can select a start time when creating a remediation task by selecting **Scheduling Assistant** on the Create New Remediation Task form.
- You can open an existing remediation task and schedule from there.

The Scheduling Assistant uses the time slots from the equipment model entity schedules. For more information, see Managing an equipment model entity schedule.

Procedure

1. If you want to select a start time while creating a remediation task, do these actions:
   a. Refer to Create a remediation task and complete steps 1-6.
   b. Select **Scheduling Assistant**.
   c. Select the date and time slot when you'd like the remediation task to take place.



   d. Select **Schedule**.

2. If you want to select a start time for an existing remediation task, do these actions:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Navigate to **All** > **Industrial Workspace**.

b. In the list view, navigate to **OT Remediation Tasks** > **Assigned to me**.

c. From the list, select the remediation task that you want to set a start time for.

d. Select **Scheduling Assistant**.

e. Select the date and time slot when you'd like the remediation task to take place.

f. Select **Schedule**.

Result
The remediation task takes place during the set time.

Split remediation task

User can split the Vulnerable items (VIs) from a remediation task record to create a remediation task.

Before you begin
Role required: sn_otvr.remediation_owner

Procedure

1. Navigate to **All** > **Industrial Workspace** > **OT Remediation Tasks** > **Assigned to Me**.
2. From the list, select the VIs that you want to move to a new remediation task.
3. Click **Split Task**.
4. In the dialog that is displayed, fill the short description field.

   The number of VIs you selected from the list is displayed.
5. In the dialog box, select **Split Task** again.

View remediation tasks in the Industrial Workspace

View the remediation tasks created for the Operational Technology (OT) vulnerable items (VITs) in the Industrial Workspace.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace** > **List menu (**  **)** > **OT Remediation Tasks**.
2. View all the remediation tasks assigned to you by selecting the **Assigned to me** list.
3. View all the remediation tasks assigned to the user groups that you are assigned to as a user by selecting the **Assigned to My Groups** list.
4. View the remediation tasks that you have requested to be considered as exceptions by selecting the **My Exception Requests** list.
5. View all the remediation tasks in your OT environment that have been approved as exceptions by selecting the **All Exceptions** list.
6. View all the remediation tasks created in the OT environment by selecting the **All** list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Create a remediation task

Split remediation task

Defer a remediation task

Defer a remediation task to create an exception request that you can resolve later.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. To open the Industrial Workspace list view, select the list () icon.
3. Under the **OT Remediation Tasks** module, select one of the available lists.
4. Select the remediation task that you want to defer.
5. Select **Request Exception**.
6. On the form, fill in the fields.

Field	Description
Until	Select the date when the Deferred state expires and the remediation task is reactivated.
Reason	Enter the reason for deferring the issue. Choices include: ○ Awaiting maintenance window ○ False positive ○ Fix unavailable ○ Risk accepted ○ Mitigating control in place ○ Other
Additional information	Enter any other relevant information.

7. Select **Save**.

Result

An exception request is created. You can view your exception requests in the **My Exception Requests** list under the **OT Remediation Tasks** module. You can also view all existing exception requests in the **All Exceptions** list under the **OT Remediation Tasks** module.

Understanding compensating controls for Operational Technology

Compensating controls in OT environments are alternative security measures when risks posed by vulnerabilities can't be patched immediately.

In OT environments, systems often cannot be taken offline for updates due to their critical role in infrastructure and production processes. Compensating controls secures the OT environment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and reduces the risk until the vulnerability can be fully remediated using permanent solutions, such as patches or hardware replacements.

The following table describes certain scenarios where compensating controls helps in reducing risk:

Use cases scenarios for compensating controls

Use case scenario	Compensating controls
Unauthorized access to programmable logic controllers (PLCs).	• Implement access control lists (ACLs) on network devices. • Disable unused ports and services on PLCs. • Implement strong passwords and authentication mechanisms.
Buffer Overflow in Human Machine Interfaces (HMI) Panels	• Apply firmware updates released by HMI panel manufacturer. • Enable hardware watchdog timers for fail-safe operations. • Implement boundary checks in the application code.
Man-in-the-Middle Attacks on PROFINET	• Use encrypted communications via VPNs or IPsec. • Configure PROFINET with secure certificates. • Implement network segmentation with firewalls.
Denial of Service (DoS) on SCADA Systems	• Enable rate-limiting on critical OT network components. • Configure SCADA systems for redundancy and load balancing. • Apply security patches provided by Siemens.
Malware Infection on Engineering Workstations	• Install and regularly update manufacturer recommended anti-malware software. • Apply application allow list to prevent unauthorized software execution. • Use secure removable media policies.

Use compensating controls for Operational Technology

Configure compensating controls for Operational Technology (OT).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

Compensating controls help mitigate the likelihood or impact of a successful exploit. For more information about compensating controls, see Understanding compensating controls for risk reduction.

Before you begin

Role required: sn_vul.vulnerability_admin or sn_vul.vulnerability_analyst

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the List () icon.
3. Under the **Libraries** module, select the **Compensating Controls** list.
4. Select **New**.
5. On the form, fill in the following fields.

Compensating Controls form

Field	Description
Name	The name of the compensating control you want to add.
Description	An explanation of the compensating control you want to add.
Active	If selected, the compensating control is activated.

6. Select **Save**.

View Common Vulnerability Entries in the Industrial Workspace

View Common Vulnerability Entries (CVEs) in the Industrial Workspace to access information needed for compensating controls.

Before you begin

Role required: sn_vul.vulnerability_admin

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the List () icon.
3. Under the **Libraries** module, select the **CVEs** list.

Operational Technology Vulnerability Response reference

Reference topics provide additional information about the Operational Technology Vulnerability Response application.

Components installed with Operational Technology Vulnerability Response

Several types of components are installed with activation of the Operational Technology Vulnerability Response (com.sn_otvr) plugin, including user roles and a business rule.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

Roles installed

Role title [name]	Description	Contains roles
OT Vulnerability Remediation Owner [sn_otvr.remediation_owner]	Can create remediation tasks. Can also schedule existing remediation tasks for vulnerable items.	• cmdb_ot_isa_viewer • cmdb_ot_viewer • sn_vul.close_vi_vg • sn_vul.remediation_owner
OT VR Integration Viewer [sn_otvr.integration_viewer]	Can view Operational Technology Vulnerability Response integration records.	None
OT VR Integration Admin [sn_otvr.integration_admin]	Can view and edit Operational Technology Vulnerability Response integration records.	• sn_sec_cmn.admin • sn_otvr.integration_viewer • sn_vul.read_all

Business rules installed

Business rule	Table	Description
Associate OT VITs To Remediation Task	Remediation Task [sn_vul_vulnerability]	When an OT Remediation task is created, groups the associated vulnerable items to the task with respect to the filter condition specified in the task->Filter grouping configuration.

Operational Technology Vulnerability Response vulnerable item form fields

List of fields displayed in a vulnerable items created for OT devices.

Vulnerable item fields

Field	Description
Overview	
Number	Automatically generated vulnerable item number for this record.
State	This field defaults to **Open**, but you can change it to **Under Investigation** if the vulnerability is ready for immediate remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Risk rating	Quantified **Risk Score** separating vulnerable items into Critical, High, Medium, Low, and None. For more information on risk ratings, see Vulnerability Response calculators and vulnerability calculator rules. **Note:** This base **Risk rating** isn't the same as the Solution record **Risk rating.**
Risk score	Calculated amount of risk the vulnerable item poses to your environment. **Note:** This base **Risk score** isn't the same as the Solution record **Risk score.** For more information, see Vulnerability Response calculators and vulnerability calculator rules.
Vulnerability	ID of the vulnerability associated with this vulnerable item.
Source	Scanner that found this vulnerable item.
Configuration item	ID of the OT asset associated with this vulnerable item.
Assignment group	Group selected to work on this remediation task.
Assigned to	Individual from the selected assignment group that works on this vulnerability.
Created	Date this vulnerable item was created in your instance.
Last opened	Date the vulnerable item was most recently opened in your instance. Initially, this is the same as the creation date of the vulnerable item, however, if it was closed, then reopened the Last opened date contains the date and time reopened.
Updated	Date of the last scan.
Summary	Description of the vulnerability.
Severity	Normalized degree of severity of this vulnerability. Severity maps are provided for NVD and with ServiceNow third-party integrations. For more information on creating or adjusting severity maps, see .Create a Vulnerability Response severity map.
Vulnerability score (v3)	CVSS v3 score.
Vulnerability score (v2)	CVSS v2 score.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Exploit exists	Yes, if at least one exploit is associated with the vulnerabilities associated with this vulnerable item.
Exploit attack vector	Most vulnerable attack vector of the exploits for the vulnerabilities associated with this vulnerable item.
Exploit skill level	Lowest skill level required to exploit the vulnerabilities associated with this vulnerable item.
Date published	Date the vulnerability was published.
Last modified	Date the vulnerability was last modified.
Threat	Relevant information about the threat. Pulled from the vulnerable entry record. **Note:** Any changes made here update the vulnerable entry record.
Remediation notes	Relevant solution to the threat, pulled from the vulnerable entry record.
Additional comments/Work notes	Any relevant information. Select the check box to add Additional comments. Starting with Vulnerability Response v20.0, you can add work notes in the Notes section for a deferred vulnerable item.
Activity	Only appears when a work note has been created.
Related Links	
Calculate Risk Score	When either the **Vulnerability Severity** or **Risk Score** calculators is enabled, the **Risk Score** field is updated.

Related information

Find more information about the Network Intrusion Detection System (NIDS) extension class, OT extension classes, and related applications.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Network Intrusion Detection System (NIDS) CI extension class

The Network Intrusion Detection System (NIDS) [cmdb_ci_nids] class builds the relationships between passive network monitoring appliances, and the devices on the network that it discovers.

Operational Technology (OT) extension classes

The Configuration Management Database (CMDB) updates classes for OT.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related applications

Vulnerability Response

When integrated with Operational Technology Vulnerability Response, the ServiceNow Vulnerability Response application aids you in prioritizing and resolving OT vulnerabilities based on process criticality.

CMDB CI Class Models app

The CMDB CI Class Models store app adds class models that extend the CMDB class hierarchy, including class descriptions, identification rules, identifier entries, and dependent relationships.

Industrial Process Manager

Use the Industrial Process Manager application to create the ISA-95 Equipment Model data foundation that is required for the ServiceNow Industrial solution, enabling you to create your own version of the equipment models in each of your industrial sites.

Operational Technology Manager

The Operational Technology Manager application enables you to aggregate OT device data from multiple sources, so that you can build the foundational data relationships used in the Industrial solution.

Operational Technology Incident Management

Operational Technology Incident Management enables manufacturers to manage OT device incidents from open to closure.

Explore  Exploring Operational Technology Incident Management	Configure  Plan and configure your implementation
Use  Using Operational Technology Incident Management	Reference  Get details about related information and applications

Exploring Operational Technology Incident Management

Learn more about the Operational Technology Incident Management application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Incident Management overview

Watch an overview about the Operational Technology Service Management product suite to learn more about the Operational Technology Incident Management application.
https://player.vimeo.com/video/1019801515?badge=0&autopause=0&player_id=0&app_id=58479

Key features

With Operational Technology Incident Management, you can use the following key features.

- Create OT incidents and drive workflows to quickly restore production processes impacted by OT devices.
- Understand context and impact of OT incidents on production processes.
- Monitor and manage OT incidents separately from IT incidents.
- Assign a separate role for the OT incident fulfiller.
- Improved OT user experience.
- Support for Operational Technology Knowledge Management. For more information, see Operational Technology Knowledge Management.

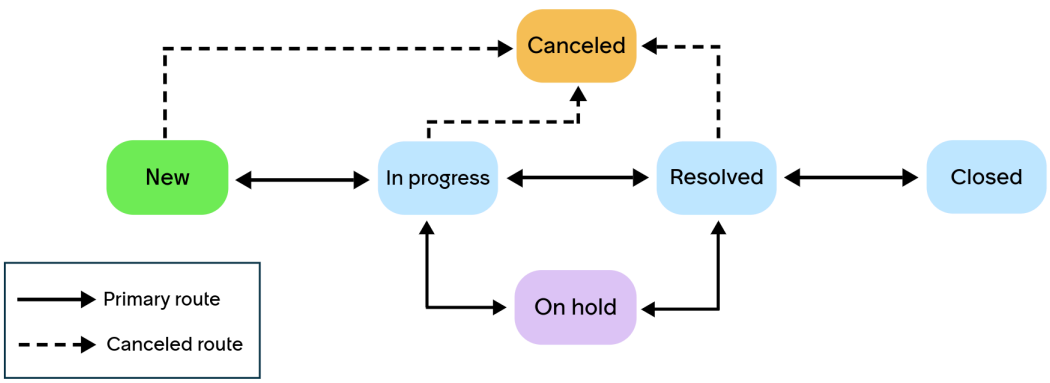
Operational Technology Incident Management

Operational Technology Incident Management enables engineers to quickly resolve Operational Technology (OT) device and production process issues.

Operational Technology Incident Management enables you to manage OT incidents separately from IT incidents. OT incidents occur when there's a disruption in service provided by an OT device on an OT network. Sometimes, the OT device may not be known when the incident is first created. If the OT device is unknown, an incident can be raised for an equipment model entity where the issue occurred.

The OT Incident manager is responsible for managing the default life cycle of incidents from creation to closure. The OT Incident Management process has many states, and each is important to the success of the process and the quality of service delivered. The different states are shown in the following diagram.

Operational Technology Incident Management process states



The incident states are as follows.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State	Description
New	Incident is logged but not yet investigated.
In Progress	Incident is assigned and being investigated.
On Hold	The responsibility for the incident temporarily shifts to another entity to provide further information, evidence, or a resolution. When you select the **On Hold** option, the following **On hold reason** list appears. These list options call out where your additional information is coming from. • Awaiting Caller • Awaiting Change • Awaiting Problem • Awaiting Vendor If the On Hold reason is **Awaiting Caller**, the **Additional comments** section is required. **Note:** If the caller updates the incident, the On Hold reason field is cleared and the state of the incident is changed to **In Progress**. An email notification is sent to the user whose name is mentioned in the **Assigned to** field and the users on the Watch list. You can place an incident On Hold one or more times before closing the incident.
Resolved	An acceptable fix is provided for the incident to ensure that it doesn't happen again.
Closed	Incident is marked **Closed** after it's in the **Resolved** state for a specific duration, and it's confirmed that the incident is satisfactorily resolved.
Canceled	Incident was triaged but found to be a duplicate incident, an unnecessary incident, or not an incident at all.

Integrating with Industrial Process Manager

Integrate Operational Technology Incident Management with Industrial Process Manager to report incidents on equipment model entities.

Industrial Process Manager creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Operational Technology solution. When integrated with Operational Technology Incident Management, you're enabled to view incident impact against production processes.

The ISA Equipment Model plugin (sn_isa_model) installed with Industrial Process Manager enables views for specified roles. For more information, see ISA-95 equipment model.

When an OT incident is created from an OT device record, the following occurs:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The **OT device** field on the OT incident form is filled with the OT device value.
- If the OT device has an associated equipment model entity, then the equipment model entity is added to **Equipment model entity** field on the OT incident form.
- The **Site** field on the OT incident form is filled with the site of the OT device.

When an OT incident is created from an equipment model entity record, the following occurs:

- The **Equipment model entity** field on the OT incident form is filled with the equipment model entity value.
- The **Site** field on the OT incident form is filled with the site of the equipment model entity.

The **OT incident** related list on the equipment model entity record shows all OT incidents reported on that entity. The **Equipment model entity** field on the form can only have entities under the selected site.

ServiceNow Otto for Operational Technology (OT) Service Management

The ServiceNow Otto for Operational Technology (OT) Service Management application enables teams to summarize OT incident details and generate incident resolution notes to share with other users.

ServiceNow Otto for OT Service Management overview

The following generative AI capabilities are available for OTSM users:

- An auto-generating OT incident summary that helps you understand the OT incident context.
- Auto-generated OT incident resolution notes that help other users resolve similar incidents.

Note: Depending on your license, you will have access to certain application features, generative AI skills, agentic workflows, and AI agents. For more information, see ServiceNow product tiers.

ServiceNow Otto for OT Service Management skills

Operational Technology (OT) incident summarization

Enables you to expedite the OT incident troubleshooting process by reviewing a summary that includes the issue, actions taken, and resolution. You can generate an incident summary for active incidents to understand the incident context. You can also refresh the summary, post the summary to the incident work notes, copy the summary, and provide feedback about the summary.

The incident summary includes the following information:

- Short description
- Description
- Work notes
- Additional comments
- Priority
- Site
- Equipment model entity
- OT device
- OT incident task

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Resolution note generation for OT incidents

Automatically generates the resolution notes for an OT incident and provides the context to another user who might encounter similar incidents.

Availability notices

Important:

- Not all model providers are available for customers with in-country SKUs, and some AI products/features are currently unavailable for in-country customers. For more information, see the KB1584492 article in the Now Support Knowledge Base. Be sure to check for model provider availability updates in future releases.
- Some AI products/features are currently unavailable for customers in the FedRAMP, NSC DOD IL5, or Australia IRAP-Protected data centers, self-hosted customers, or in other restricted environments. For more information, see the KB0743854 article in the Now Support Knowledge Base. Be sure to check for availability updates in future releases.
- Some AI products/features are currently available only for customers in some regions. Be sure to check for availability updates in future releases.
- Some AI products and skills are not available in Regulated Markets. For more information, see KB2593939: Regulated Markets AI Products/Skills Not Available. Be sure to check for availability updates in future releases.

Troubleshoot and get help

- ServiceNow Community on AI and Intelligence
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

AI limitations

This application uses artificial intelligence (AI) and machine learning, which are rapidly evolving fields of study that generate predictions based on patterns in data. As a result, this application may not always produce accurate, complete, or appropriate information. Furthermore, there is no guarantee that this application has been fully trained or tested for your use case. To mitigate these issues, it is your responsibility to test and evaluate your use of this application for accuracy, harm, and appropriateness for your use case, employ human oversight of output, and refrain from relying solely on AI-generated outputs for decision-making purposes. This is especially important if you choose to deploy this application in areas with consequential impacts such as healthcare, finance, legal, employment, security, or infrastructure. You agree to abide by ServiceNow's AI Acceptable Use Policy, which may be updated by ServiceNow.

Data processing

This application requires data to be transferred from ServiceNow customers' individual instances to a centralized ServiceNow environment, which may be located in a different data center region from the one where your instance is, and potentially to a third-party cloud provider, such as Microsoft Azure. This data is handled per ServiceNow's internal policies and procedures, including our policies available through our CORE Compliance Portal.

Data collection

ServiceNow collects and uses the inputs, outputs, and edits to outputs of this application to develop and improve ServiceNow technologies including ServiceNow models and AI products. In addition, this application will collect incident data (for Incident Assist and Knowledge Assist) and chat transcripts (for Chat Assist). Customers can opt out of future data collection at any time, as described in the Now Assist Opt-Out page.

For more information, see the Now Assist documentation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuring Operational Technology Incident Management

Configure the Operational Technology Incident Management application so that you can create the data foundation for the ServiceNow® Operational Technology solution.

Operational Technology Incident Management v2 is dependent on Tokyo P5 or later.

Note:

If you have the admin role, you can use the Guided Setup to lead you through the setup of the Operational Technology Incident Management application. To access the Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

Task	Purpose
1. Install the Operational Technology Incident Management application from the ServiceNow Store.	Installs the Operational Technology Incident Management application and supporting plugins.
2. Assign Operational Technology Incident Management roles.	Assigns roles to control the actions that are available for each user.
3. Migrate OT Incidents.	Migrates OT incidents from the incident table to the OT incident table. **Note:** This step applies only when upgrading from Paris, San Diego, or Tokyo to Utah.
4. Configure categories and subcategories for OT incidents.	Configures categories and subcategories for OT incidents as needed.
5. Configure state models.	Configures state models for OT incident sites.
6. (Optional) Create an assignment rule.	Create an assignment rule to automatically assign an OT incident to the right group or user.

Configure ServiceNow Otto for Operational Technology (OT) Service Management

If you have the admin role, you can configure the ServiceNow Otto for Operational Technology (OT) Service Management application so that teams can use the generative AI capabilities in the Industrial Workspace for their OT incidents.

Before you begin

Role required: admin

About this task

Use the AI Admin Hub console to configure ServiceNow Otto for OT Service Management. The console helps you install plugins and configure generative AI skills. For more information, see Overview tab in AI Admin Hub.

You can also set up AI Enhanced Recommended Actions for OTSM to use with ServiceNow Otto for OT Service Management. For more information, see Set up AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: Some generative AI skills, AI agents, and agentic workflows are turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

The following table lists the features and skills that you can access from the AI Admin Hub console.

OTSM features and skills in the AI Admin Hub console

OTSM features	Skills
Gen AI skills for OT incident	• OT resolution notes generation • OT incident summarization **Note:** The incident summarization is applicable only for incidents in the New, In progress, On-hold, Resolved, or Closed states as long as the incident state mappings that are provided in the base system aren't customized.

Procedure

1. Activate the ServiceNow Otto for OT Service Management plugin (sn_otsm_gen_ai).
   - For information about the application dependencies, see Supporting information for ServiceNow Otto for Operational Technology (OT) Service Management.
   - For information about the installation process, see Install plugins.
2. Navigate to **All** > **AI Admin Hub**.
3. Select the **AI Skills** tab.
4. Activate and configure the skills for the ServiceNow Otto for OT Service Management features. These features are grouped under the **Technology** workflow group. Each feature has its associated skills.
5. On the tile for your skill, select **Activate skill**.
6. Select the inputs or triggers for the selected skill.

   For information about the inputs and triggers for each skill, see Skill inputs and triggers for ServiceNow Otto for Operational Technology (OT) Service Management.
7. After you configure the inputs or triggers, select **Save and continue**.
   You can return to a previous step by using the **Back** button.
8. Define access as needed to determine who can access the selected skill.

   Note: For both the OT incident summarization skill and the OT incident resolution notes generation skill, a user must have the sn_ot_incident_write role.
9. After you configure the access controls, select **Save and continue**.
10. Select where to display the skill.
    - **In-product**: When selected, the AI skills are displayed on forms and workspaces.
    - **ServiceNow Otto panel**: When selected, the AI skills are available in the ServiceNowOtto panel. If you don't see this option, you must activate the panel. For more information, see Activate the panel in standard chat.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

11. After you configure the display for the selected skill, select **Save and continue** to go to the next step.
12. Review your choices and select **Activate** to complete the configuration.

Supporting information for ServiceNow Otto for Operational Technology (OT) Service Management

Review the supported language models, supported interfaces, and application dependencies for ServiceNow Otto for Operational Technology (OT) Service Management.

Supported language models for all ServiceNow Otto for OT Service Management skills and AI agents

You can use Now LLM Service, Azure OpenAI, Google Gemini or Anthropic Claude on AWS as the AI model provider for all generative AI skills and AI agents. Use the Configuration Controls in AI Control Tower to define which options are available, then set the skill-level preferences in the AI Admin Hub console. For more information, see Large language models on the ServiceNow AI Platform.

Supported user interfaces

The ServiceNow Otto for OT Service Management application includes the skills that are listed in the following table.

Note: Depending on your license, you will have access to certain application features, generative AI skills, agentic workflows, and AI agents. For more information, see ServiceNow product tiers.

ServiceNow Otto for OT Service Management supported interfaces

Interface	Skill
Industrial Workspace	• OT incident summarization • OT resolution notes generation

Skill inputs and triggers for ServiceNow Otto for Operational Technology (OT) Service Management

Skill inputs and triggers for ServiceNow Otto for Operational Technology (OT) Service Management determine how and when each skill is used. Configure inputs to identify the data a skill uses, or configure triggers to initiate skill actions.

ServiceNow Otto for OT Service Management skill input overview

Depending on the selected skill, you can configure the inputs or triggers. These settings determine how and when a skill is used. An input identifies the data used for a skill, such as the table and fields used to generate an incident summary. A trigger initiates an action, such as when the system generates OT resolution notes.

OT incident summarization skill

The OT incident summarization skill includes the inputs that identify the table and fields that are used when an OT incident summary is generated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: This generative AI skill is turned on by default. The skill will be automatically available to appropriate role users for the application. For more information, see AI agents, skills, and agentic workflows on by default.

The following table lists the inputs for the OT incident summarization skill.

Inputs for the OT incident summarization skill

Input	Description
Input table	OT incident [sn_ot_incident]
Input fields	• Description • Short description • Work notes • Additional comments • Priority • Site • Equipment model entity • OT device • OT incident task
Input template states	• New • WIP • Resolved • Closed

The following table lists the descriptions for the OT incident summarization skill.

Descriptions for the OT incident summarization skill

Description	Mandatory for input state
Issue	• New • WIP • Resolved • Closed
Key Actions Taken	• WIP • Resolved • Closed

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Descriptions for the OT incident summarization skill (continued)

Description	Mandatory for input state
Resolution	• Resolved • Closed
OT incident task	• WIP • Resolved • Closed

OT resolution notes generation skill

The OT resolution notes generation skill includes the inputs that identify the table and fields that are used when the resolution notes are generated for an OT incident.

Important: This generative AI skill is turned on by default. The skill will be automatically available to appropriate role users for the application. For more information, see AI agents, skills, and agentic workflows on by default.

The following table lists the inputs for the resolution notes generation skill.

Inputs for the OT resolution notes generation skill

Input	Description
Input table	OT incident [sn_ot_incident]
Input fields	• Description • Short description • Work notes • Additional comments • Priority • Site • Equipment model entity • OT Device

Install Operational Technology Incident Management

You can install the Operational Technology Incident Management application (sn_ot_inc_mgmt) if you have the admin role. The application installs related ServiceNow® Store applications and plugins if they are not already installed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- Operational Technology Incident Management requires the following plugins. Ensure that these plugins are activated before you install Operational Technology Incident Management.

  Required ServiceNow plugins

  CMDB CI Class Models (sn_cmdb_ci_class)

  The CMDB CI Class Models store app adds class models that extend the CMDB class hierarchy, including class descriptions, identification rules, identifier entries, and dependent relationships. For more information, see CMDB CI Class Models store app.

  ISA Equipment Model (sn_isa_model)

  The data model for ISA-95 equipment model entities and templates. For more information, see ISA-95 equipment model.

- Operational Technology Incident Management requires either one or both of the following ServiceNow Store applications. Ensure that at least one of these applications is installed before you install Operational Technology Incident Management.

  Required ServiceNow Store applications

  Operational Technology Manager

  The Operational Technology Manager application creates the foundational data and relationships that enables your enterprise to use the ServiceNow® Operational Technology solution. Operational Technology Manager supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the ServiceNow AI Platform. For more information, see Configuring the Operational Technology Manager.

  Industrial Process Manager

  The Industrial Process Manager application creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Industrial solution, enabling you to create your own version of the equipment models in each of your industrial sites. For more information, see Configure the Industrial Process Manager.

- Role required: admin

About this task

The following items are installed with Operational Technology Incident Management:

- Plugins
- Store applications
- Roles and ACLs

For more information about the roles and ACLs installed, see Components installed with Operational Technology Incident Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: For Operational Technology Service Management users with no license for Operational Technology Visibility, note the following:

- When you have the latest version of Operational Technology Incident Management installed, Industrial Process Manager is also installed.
- When you have the latest version of Operational Technology Change Management installed, Industrial Process Manager is also installed.

You should upgrade to the latest versions so you have access to the Operational Technology Service Management experience.

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Operational Technology Incident Management application (sn_ot_inc_mgmt) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find the application, you might have to request it from the ServiceNow Store.

   Visit the ServiceNow Store to view all the available apps, and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.
3. In the Application installation dialog box, review the application dependencies.

   Dependent plugins and applications are listed if they will be installed, are currently installed, or need to be installed. If any plugins or applications need to be installed, you must install them before you can install Operational Technology Incident Management.
4. Select **Install**.

Migrate incidents to the new incident table

Migrate Operational Technology incidents from the old incident table to the new incident table. Migrating incidents lets the Operational Technology Incident Management application know that the old table is no longer applicable.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin

Procedure

1. Navigate to **Industrial Workspace Admin** > **Guided Setup**.
2. In the Operational Technology Incident Management category, select **Get Started**.
3. Next to the Migrate OT Incidents section, select **Configure**.
4. Start the migration by selecting **Execute now**.
5. **Optional:** To see the activity log for this scheduled job, navigate to **All** > **System Logs** > **System Log** > **All**.

Result

The Operational Technology incidents are migrated to the new incident table, and the Operational Technology Incident Management application no longer uses the old table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign roles to your users

Assign roles to your users in the Operational Technology Incident Management application so that you can control their access to the features, capabilities, and data.

Before you begin

Role required: admin or user_admin

About this task

Users with the roles that are listed in the following table can use the Operational Technology Incident Management application.

Note: The OT Incident User [ot_incident_user] role is deprecated. For users who are assigned with this role, you can execute the scheduled job "Assign New OT Incident Roles" to assign them with new Operational Technology Incident Management roles. For more information, see Assign new roles to your users.

Role	Description
OT Incident Admin [sn_ot_incident_admin]	Can create, view, delete, and edit OT incident records for any equipment model entities. Users with this role can configure **Priority Lookup Rules** and **OT incident system properties**.
OT Incident Reader [sn_ot_incident_read]	Can only view OT incident records.
OT Incident Fulfiller [sn_ot_incident_write]	Can create, view, and edit OT incident records.

Procedure

Assign roles to users or groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Assign new roles to your users

Assign new roles to users who had the OT Incident User [ot_incident_user] role through a scheduled job in the Operational Technology Incident Management application.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin or user_admin

About this task

The OT Incident User role [ot_incident_user] is deprecated. You can assign new roles to users that had the ot_incident_user role through a scheduled script execution.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
2. In the search bar, search for the **Assign New OT Incident Roles** scheduled job.
3. Start a scheduled job by selecting **Execute now**.
4. **Optional:** To see the activity log for this scheduled job, navigate to **All** > **System Logs** > **System Log** > **All**.

Result

The scheduled job is executed and users are now assigned with the new Operational Technology Incident Management roles.

Create an assignment group

Create an Operational Technology (OT) specific assignment group to assign to OT incident records.

Before you begin

Role required: admin

About this task

The **Assignment Group** field in an OT incident record only shows assignment groups with the type OT. This helps separate Operational Technology (OT) and Information Technology (IT) incidents.

You can create OT-specific assignment groups that you want visible on an OT incident record.

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. Select **New**.
3. On the form, fill in the fields.

Assignment groups form

Field	Description
Name	Name of the assignment group.
Manager	Group manager or lead.
Type	Category for this group. In the **Select target record** field, search for **OT** to add it to the type field.
Group email	Group email distribution list or the email address of the point of contact.
Parent	Other group that the group is a member of.
Description	Description of the assignment group.

4. Select **Submit**.

Result

Now, the OT-specific assignment group is visible on the incident record.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incident categories and subcategories

By categorizing Operational Technology (OT) incidents, you can group and narrow the search for specific OT incidents.

When you can create an OT incident, you can choose from the categories and subcategories that are listed in the following table.

Incident categories

Category	Subcategory
Database	• DB2 • MS SQL Server • Oracle
Hardware	• OT issue • CPU • Disk • Keyboard • Memory • Monitor • Mouse
Inquiry / Help	• Antivirus • Email • Internal Application
Network	• DHCP • DNS • IP Address • VPN • Wireless
Productivity	• Minor Stops • Slow Running • Setup and Adjustments • Breakdown
Quality	• Incoming Material • Startup Rejects

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incident categories (continued)

Category	Subcategory
	• Process Defects - Qualitative • Process Defects - Quantitative
Safety	• Near Miss • Hazard • Safety Concern • Accident
Software	• Email • Operating System

Edit a category or subcategory

Edit your existing Operational Technology incident categories and subcategories to classify your incidents.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin or sn_ot_incident_admin

Procedure

1. Navigate to **All** > **System Definition** > **Choice Lists**.
2. Set the condition filters to **[Table] [is] [sn_ot_incident]** and **[Element] [is] [category]** or **[Element] [is] [subcategory]**.
3. Select the category or subcategory record.
4. Edit the form based on your needs.
5. Select **Save**.

Result

Now, the changes to the existing category or subcategory appear on the record.

Create a category or subcategory

Create an Operational Technology incident category or subcategory that you want to use to classify incidents.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin or sn_ot_incident_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Definition** > **Choice Lists**.
2. To create a category, do these actions:
   a. Select **New**.
   b. In the **Element** field, enter the word `category`.
   c. In the **Label** field, enter the category name.
   d. In the **Value** field, enter the category value.
   e. In the **Sequence** field, enter the sequence number.
   f. Select **Submit**.
3. To add a new subcategory, do these actions:
   a. Select **New**.
   b. In the **Element** field, enter the word `subcategory`.
   c. In the **Label** field, enter the subcategory name.
   d. In the **Value** field, enter the subcategory value.
   e. In the **Sequence** field, enter the sequence number.
   f. If the subcategory belongs to an existing category, add the category value to the **Dependent value** field.
   g. Select **Submit**.

Result

The new category or subcategory is available to select on an Operational Technology incident record.

Delete a category or subcategory

Delete an Operational Technology incident category or subcategory if your organization no longer uses that category or subcategory.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin or sn_ot_incident_admin

Procedure

1. Navigate to **All** > **System Definition** > **Choice Lists**.
2. Set the condition filters to **[Table] [is] [sn_ot_incident]** and **[Element] [is] [category]** or **[Element] [is] [subcategory]**.
3. Point to the category or subcategory record that you want to delete and select the check box.
4. In the Actions on selected rows menu, select **Delete**.

Result

The deleted category or subcategory is no longer available on an Operational Technology incident record.

Create an incident state model

Create an Operational Technology (OT) incident state model for your sites. By using an incident state model, you can manage the life cycle of the related incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin

- Set the application scope to **Operational Technology Incident Management**.
- Role required: admin or state_model_admin

About this task

By using state management, you can configure a state model for OT incident sites and their incident life cycles. You can create one model per site.

For more information about state management and state models, see State Management.

For more information about the incident life cycles, see Operational Technology Incident Management.

Procedure

1. Navigate to **All** > **State Management** > **State Models**.
2. Select the **OT Incident: Default Flow** model.
3. Set the **Condition**.
4. In the State Transitions Context menu, configure the State Transition records as required. For example, if you want to edit the **Enter Condition** field of the **In Progress** state record, select the state record, add your changes, and select **Update**.
5. Select **Update**.

Result

Now, the state model accurately describes the expected record workflow through the life cycle of the incident record.

Define a priority lookup rule for incidents

Define the impact and urgency of an Operational Technology incident to calculate its priority. You can then use the priority calculation to prioritize your work and to drive service level agreements (SLAs) in your organization.

Before you begin

Role required: ot_incident_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Operational Technology Incident Management** > **Priority Lookup Rules**.
2. Select **New**.
3. On the form, fill in the fields.

Priority lookup rule form

Field	Description
Impact	Measure of the effect of an incident on business processes.
Urgency	Measure how long the resolution can be delayed until an incident has a significant business impact.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Priority	Option that is based on the impact and urgency. The priority identifies how quickly the OT engineer should address the task.
Application	Scope of the rules. The scope defines whether the rules are available for all applications or for scoped applications.
Active	Option to define whether the rule is active or not.
Order	Order in which the rules appear in the priority lookup list. This field indicates which rule to execute first.

Note:

The priority is calculated according to the sample data lookup rules in the following table.

Priority Data lookup rules

Impact	Urgency	Priority
1 - High	1 - High	1 - Critical
1 - High	2 - Medium	2 - High
1 - High	3 - Low	3 - Moderate
2 - Medium	1 - High	2 - High
2 - Medium	2 - Medium	3 - Moderate
2 - Medium	3 - Low	4 - Low
3 - Low	1 - High	3 - Moderate
3 - Low	2 - Medium	4 - Low
3 - Low	3 - Low	5 - Planning

By default, the **Priority** field is read-only and must be set by selecting the **Impact** and **Urgency** values. To change how the priority is calculated, you can either alter the priority lookup rules or disable the **Priority is managed by Data Lookup - set as read-only** UI policy and create their own business logic.

4. Select **Submit**.

Set the system properties

Set the system properties for the Operational Technology Incident Management application so that you can enable the incident properties as needed.

Before you begin

- Set the application scope to **Operational Technology Incident Management** by selecting the Globe icon ( ) in the navigation bar.
- Role required: sn_ot_incident_admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Operational Technology Incident Management** > **System Properties**.
2. Enable the following properties as needed for your organization.

Property	Description
com.sn_ot_inc_mgmt.sn_ot_incident_task.closure	Property to close the open OT incident tasks when the related incident is closed or canceled. If you want to close the open incident tasks when the related incident is closed or canceled, set this field to **Yes**.
com.snc.sn_ot_incident.create.child.enable	Property to create a child incident feature for the OT incident records. If you want to create a child incident for incident records, set this field to **Yes**.
com.snc.sn_ot_incident.copy.attributes	Property to list the attributes that you want to copy from the parent incident to the child incident. Add any additional attributes needed in the comma-separated list.
glide.ui.sn_ot_incident_activity.fields	Fields that are visible in the activity formatter. Add any additional fields needed in the comma-separated list.

3. Select **Save** to save your changes.

Create an assignment rule

Create an assignment rule to automatically assign an Operational Technology (OT) incident to a group or user according to one or more conditions in the assignment rule. You use assignment rules to run at the time that you open an OT incident.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **System Policy** > **Rules** > **Assignment**.
2. Select **New**.
3. On the form, fill in the fields.
   For a description of the field values, see Assignment rule form.
4. Select **Submit**.

What to do next

For more information about assignment rules, see Defining assignment rules.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using Operational Technology Incident Management

After you complete all required set up tasks for the Operational Technology Incident Management application, you can begin managing OT incidents.

Using ServiceNow Otto for Operational Technology (OT) Service Management

You can summarize an Operational Technology (OT) incident and generate OT resolution notes by using the ServiceNow Otto for OT Service Management application.

Summarize an Operational Technology incident by using ServiceNow Otto for Operational Technology (OT) Service Management

Understand the Operational Technology (OT) incident context and respond to user questions by using the OT incident summarization skill in the ServiceNow Otto for OT Service Management application.

Before you begin

Role required: sn_ot_incident_write

About this task

An OT incident summary provides you with a concise summary of an incident. The summary is based on the OT incident state and is generated from the following information:

- Short description
- Description
- Work notes
- Additional comments
- Priority
- Site
- Equipment model entity
- OT device
- OT incident task

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. On the OT Incidents module, select one of the available lists.
4. Open the OT incident record to summarize.
5. In the OT incident record, select the **Summarize** button.
6. **Optional:** Manage the OT incident summary using the available options.

Option	Procedure
Save the summary information by adding it to the incident work notes	**a.** Select **Share as Work notes**. **b.** In the Share Incident summary as Work notes dialog box, edit the summary. **c.** Select **Save to Work notes**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Option	Procedure
Expand or collapse the summary	Select the expand card icon ( ) to view the complete summary or the collapse card icon ( ) to view a collapsed summary.
Provide feedback for the summary	If the summary was helpful, select the helpful icon ( ). If the summary wasn't helpful, se lect the not helpful icon ( ). **Note:** This feedback improves the gen erative AI model and can help improve future versions of this skill.
Copy the incident summary	To reuse the summary, select the copy to clip board icon ( ).
View the information about the incident summary	To view details about the summary, select the more info icon ( ).

Generate resolution notes for an Operational Technology incident

Generate resolution notes for an Operational Technology (OT) incident to share incident resolution information with other users who encounter similar issues.

Before you begin
Role required: sn_ot_incident_write

About this task
OT incident resolution notes are generated from the following information:

- Short description
- Description
- Work notes
- Additional comments
- State
- Site
- Equipment model entity
- OT device

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. On the OT Incidents module, select one of the available lists.
4. Open the OT incident record to generate resolution notes for.
5. In the **Resolution notes** field, select the **Use AI to generate notes** quick action.
6. Select **Generate resolution notes**.
7. **Optional:** Review the resolution summary in the **Resolution notes** field and make any necessary corrections.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: AI-generated content may contain inaccuracies. Review all output before saving.

8. **Optional:** Manage the OT resolution notes using the available options.

Option	Procedure
Insert the resolution notes	To insert the generated OT resolution notes in the **Resolution note** field, select **Insert**.
Refine the resolution notes by elaborating or shortening	To provide more details in the OT resolution notes, select **Refine** and then **Elaborate**. To shorten the resolution notes, select **Shorten**.
Provide feedback for the summary	If the OT resolution notes were helpful, select the helpful icon ( ). If the resolution notes weren't helpful, select the not helpful icon ( ). **Note:** This feedback improves the gen erative AI model and can help improve future versions of this skill.
Copy the resolution notes	To reuse the OT resolution notes, select the copy to clipboard icon ( ).
View the information about the resolution notes	To view details about the OT resolution notes, select the more info icon ( ).

9. In the **Resolution code** field, update the resolution code and select **Resolve**.
   A resolution code categorizes how the incident is resolved. For example, Known error and Solved (Permanently).
   The resolution information is updated and the state of the OT incident is set to **Resolved**.

Agentic AI for Operational Technology Service Management

Use the Operational Technology Service Management (OTSM) AI agent collection to complete tasks autonomously.

Available agentic workflows for OTSM AI agent collection

Agentic workflow name	Description	Available AI agents
Generate OT KB articles	After OT incident resolution, the AI agent automatically creates a KB article with relevant contextual information.	OT knowledge generator AI agent

Important: To change this agentic workflow, duplicate it, adjust the settings to suit your specific needs, and activate the duplicated version of the agentic workflow instead.

The minimum role needed to duplicate an agentic workflow is the sn_aia.admin role. By default, the OTSM agentic workflow is inactive. To use the base system agentic workflow, activate the base system trigger. To customize the agentic workflow, duplicate it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Important: Some generative AI skills, AI agents, and agentic workflows are turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

Supported Large Language Models

Note:

You can use Now LLM Service, Azure OpenAI, Google Gemini or Anthropic Claude on AWS as the AI model provider for all generative AI skills and AI agents. Use the Configuration Controls in AI Control Tower to define which options are available, then set the skill-level preferences in the AI Admin Hub console. For more information, see Large language models on the ServiceNow AI Platform.

Security implementation considerations

Enable security implementation to execute AI agents and agentic workflows through Access Control Lists (ACLs) and user identities. For more information, see Implement access control in AI agents

Considerations for running the autonomous AI agents

Important: By default, all agent workflow and AI agent records are read-only.

To run the AI agents autonomously, you must first duplicate the agentic workflow, and then proceed with the following steps:

- Activate the agentic workflow.
- Activate all agents within the agentic workflow.
- Activate the trigger to invoke the agentic workflow automatically. The triggers for each agentic workflow must be unique. If you prefer to invoke it manually, activating the trigger isn't necessary.

Standalone AI agents

There might be AI agents installed on your instance that are not used in agentic workflows. To learn how to see all agents that are available to you, see Find AI agents.

Role masking

Agentic workflows and their AI agents use role masking to determine which users can access them. Ones installed with your applications have specific roles that come included with the application. If you select *`Users with specific roles`* for user access, you must configure the security controls to include these roles. For the instructions to change the security controls, see Define security controls for an agentic workflow.

Activate an agentic workflow for ServiceNow Otto for Operational Technology (OT) Service Management

Activate the agentic workflows for ServiceNow Otto for Operational Technology (OT) Service Management from the AI Agent Studio so that the AI agents can execute requests autonomously. The ServiceNow Otto for OT Service Management agents included with the application are activated by default.

Before you begin
Verify that the following skills are activated for ServiceNow Otto for OT Service Management:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- OT incident summarization skill
- OT resolution notes generation skill

For more information about activating the skills, see Configure Now Assist for OTSM.

Role required: sn_aia.admin

Procedure

1. Navigate to **All** > **AI Agent Studio** > **Agentic Solutions**.
2. Under the **Agentic workflows** tab, select the **Generate OT KB articles** agentic workflow.

   Important: This agentic workflow is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

3. In the **Define key requirements** screen, review and update the information as needed then select **Save and Continue**.

   Note: In the Define who can access the agentic workflow section, a user must have the sn_ot_incident_write role to access the agentic workflow.

4. In the **Add a preferred trigger** screen, confirm the **OT incident upon being resolved** trigger is set to **Active** by selecting the trigger to open the **Edit trigger** window and turning on the **Active** toggle.
5. In the **Select a UI display** screen next to the **ServiceNow Otto panel** option, select the **Display** toggle to display the conversation with the agent in the ServiceNow Otto panel.
6. Select **Save and test**.
   The agent can now execute the request for the agentic workflow.

Generate OT KB articles agentic workflow

The Generate OT KB articles agentic workflow automatically generates a KB article when an Operational Technology (OT) incident is resolved, capturing resolution information for future reference.

Generate OT KB articles overview

With the Generate OT KB articles agentic workflow, you can automatically generate a KB article for an OT incident when the state of the incident is set to **Resolved**. The article contains the following information.

Site

Site where the incident occurred.

OT Device

Affected OT device at the site.

Equipment model entity

Affected equipment model entity at the site.

Summarization

The AI-generated summary, which includes the issue, key actions taken, and OT incident tasks if applicable.

Resolution notes

AI-generated resolution notes from the OT Resolution Notes generation skill.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

KB Base

The Knowledge Base where the generated KB article is stored. The KB Base for the OTSM agentic workflow is the AI Agent OT Knowledge Base.

Author

The author that publishes the generated KB article. The author for the OT agentic workflow is the OTSM Knowledge Generator AI Agent.

The article is then automatically published and appears in the Attached Knowledge related list of the OT incident record in the Industrial Workspace. The KB Article Generation process isn't triggered if there's an article already attached to current OT incident.

To change this agentic workflow, duplicate it, adjust the settings to suit your specific needs, and activate the duplicated version of the agentic workflow instead.

Note: When you modify an agentic workflow, AI agent, or tool, verify that you update all instructions accordingly.

The minimum role needed to duplicate an agentic workflow is the sn_aia.admin role. By default, the OTSM agentic workflow is inactive. To use the base system agentic workflow, activate the base system trigger. To customize the agentic workflow, duplicate it.

AI agents used in the Generate OT KB articles agentic workflow

The OT knowledge generator AI agent is used to generate a KB article for a resolved OT incident.

Important: This AI agent is turned on by default. For more information, see AI agents, skills, and agentic workflows on by default.

Managing OT incidents

Depending on your assigned user role, you can manage OT incidents in the Industrial Workspace.

In the Industrial Workspace, the OT incident writer can create and update an OT incident form from the following places:

- An OT device form
- An equipment model entity form
- The List module

In the Industrial Workspace, the OT incident viewer can view OT incidents in the following places:

- The OT Incidents related list under the **Related Records** tab on an OT device record
- The **OT Incidents** tab on an equipment model entity record
- The following lists under the **OT Incidents** list module:
  - Assigned to me
  - Belong to my sites
  - All

The OT incident administrator can go to any OT incident record in the Industrial Workspace and delete it.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Access control for incidents

To help separate Operational Technology (OT) and Information Technology (IT) data, only OT users can view OT incidents.

The following table describes the roles and permissions for the users that have the Operational Technology Incident Management roles.

Role	Permissions
sn_ot_incident_write	Can create, edit, and read OT incidents.
sn_ot_incident_read	Can only read OT incidents.
sn_ot_incident_admin	Can create, view, edit, and delete incident records for any equipment model entity.

For more information about access control rules, see Access control rules in application administration apps.

Report an OT incident

Create an Operational Technology (OT) incident record to report a deviation from an expected standard of operation.

Before you begin

Role required: sn_ot_incident_write

About this task

For a walkthrough of how to report an OT incident, watch this video.

https://player.vimeo.com/video/1154457621?h=3e1fbdb629&badge=0&autopause=0&player_id=0&app_id=58479

Procedure

1. Navigate to the **Industrial Workspace**.
2. Select the **List** icon.
3. Under the OT Incidents list module, select one of the following available lists.
   - Assigned to me
   - Belong to my sites
   - All
4. Select **New**.
5. On the form, fill in the following the fields as needed.
   If you selected an OT device record, the **Site** and **OT device** fields are automatically filled in. If you selected an equipment model entity record, the **Site** and **Equipment model entity** fields are automatically filled in. If the OT incident is raised from the OT Incidents list module, then none of these fields are automatically filled in.

   Note: Your organization may have configured the OT incident form and its fields to adhere to your incident management process. The following table describes the typical OT incident form fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT incident form

Field	Description
Short description	Brief description of the incident.
Description	Detailed explanation of the incident.
Number	Unique system-generated incident number that is prefixed with Operational Technology Incident (OTINC).
Caller	User who contacted the OT engineer with an issue.
Impact	Measure of the effect that an incident has on industrial processes.
Urgency	Measure of how long the resolution can be delayed until an incident has a significant business impact.
State	State of the OT incident. The state moves and tracks incidents through several stages of resolution.
Category	Type of issue. After selecting the category, select the subcategory if applicable.
Subcategory	Type of issue within the selected category.
Watch list	Users who receive notifications about this incident when comments are added.
Work notes list	Users who receive notifications about this incident when work notes are added.
Site	Site where the issue happened.
OT device	Affected OT device at the site.
Equipment model entity	Affected equipment model equipment model entity at the site.
Business impact	More information about the business impact of the OT incident.
Assignment group	Assigned group that works on the incident. The assignment group can be any group with the type OT.
Assigned to	User who works on this incident. If the assignment group changes, the **Assigned to** field is cleared. You can only select the users that are included in the **Assignment group** field and have the **sn_ot_incident_write** role. If the Assignment group field is empty, then any site user with the sn_ot_incident_write role can be selected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Parent incident	Unique number of the parent incident for this incident record.
Additional comments	More information about the issue as needed. All users that can view incidents can see the additional comments.
Work notes	Information about how to resolve the incident or the steps taken to resolve it, if applicable.

6. Select **Save**.

Result
Now, the assignment group and assignee are aware that there's an OT incident that must be addressed.

What to do next
You can view an OT incident record created for an OT device directly in the device record by opening the device record, clicking the **Related Records** tab, and selecting **OT Incidents**.

Create an Operational Technology incident from an Operational Technology change request

Create an Operational Technology (OT) incident related to an OT change request directly from the OT change record in the Industrial Workspace.

Before you begin
Role required: sn_ot_change_write and sn_ot_incident_write

About this task
The following related lists are available in an OT change record in the Industrial Workspace so you can create an OT incident or add an existing OT incident related to the change request.

Incidents Fixed by Change

OT incidents that are fixed by the selected change record.

Incidents Caused by Change

OT incidents that are caused by the selected change record.

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the OT Change Requests list module, select one of the available lists.
4. Select the change record in one of your sites that you want to create an incident from.
5. To create an OT incident, complete the following actions.

   a. In the Incidents Fixed by Change related list or the Incidents Caused by Change related list, select **New**.

   b. On the form, fill in the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT incident form

Field	Description
Number	Unique system-generated incident number that is prefixed with Operational Technology Incident (OTINC).
Opened	The date the incident is submitted.
Short description	Brief description of the incident.
Site	Site where the issue happened.
Equipment model entity	Affected equipment model equipment model entity at the site.
OT Device	Affected OT device at the site.

c. Select **Save**.

6. To add an existing OT incident to the change request record, complete the following actions.

> **Note:** An OT incident can be fixed by one OT change request at most, and caused by one OT change request at most. You can add an OT incident already associated to another OT change request, but doing so overrides the existing relationship.

a. In the Incidents Fixed by Change related list or the Incidents Caused by Change related list, select **Add**.

b. Select the OT incident that you want to add.

c. Select **Add**.

Result

After you create the incident from the change request, you can view the incident record in the related list or by navigating back to the Industrial Workspace list view. Then select one of the available lists under the **OT Incidents** list module.

Create tasks to fulfill an OT incident

Create a set of incident tasks to fulfill an Operational Technology (OT) incident. Incident tasks help you to split up and categorize the work that is needed to resolve an incident.

Before you begin

Role required: sn_ot_incident_write

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. Under the OT Incidents list module, select on of the available lists.
4. Select the OT incident record that you want to create incident tasks for.
5. In the OT incident record, select the **Incident Tasks** tab.
6. Select **New**.
7. On the Create New Operational Technology Incident Task form, fill in the following fields.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Incident task form

Field	Description
Number	Unique system-generated incident task number.
Incident	Incident with which the task is related.
Site	Affected incident site. **Note:** This field is read-only and is automatically filled in with the related incident site, if applicable.
Equipment Model Entity	Affected equipment model entity. **Note:** This field is read-only and is automatically filled in with the related equipment model entity, if applicable.
OT device	Affected OT device. **Note:** This field is read-only and is automatically filled in with the related OT device, if applicable.
State	State for tracking an incident task through several stages of the incident's resolution.
Priority	Priority of the incident task.
Assignment group	Group who works on the incident task. If you leave this field empty, the incident is automatically assigned. **Note:** If needed, you can assign OT incident tasks to IT assignment groups.
Assigned to	User to whom the incident task is assigned to work on. **Note:** If the **Assignment group** changes, the **Assigned to** field is cleared.
Short description	Brief description of the incident task.
Description	Detailed explanation on the incident task.
Notes	
Work notes list	Users who receive notifications about this incident task when work notes are added.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Note: You can also add yourself to the work notes list.
Work notes	Information about how to resolve the incident task, or the steps that need to be taken to resolve it, if applicable.

8. Select **Save**.

Result
You can view incident tasks in the Industrial Workspace list view in the following places.

- Incident tasks assigned to you: **OT Tasks** > **Assigned to Me**
- Incident tasks assigned to your group: **OT Tasks** > **Assigned to My Groups**
- Unassigned incident tasks: **OT Tasks** > **Unassigned**

Create a child incident

Create a child Operational Technology (OT) incident record to capture part of the deviation reported so that it can be worked on separately. Creating child incidents can help you organize multiple incidents related to the same parent.

Before you begin

- Enable the Create child incident feature (*com.snc.incident.create.child.enable*) property. For more information, see Set the system properties.
- Role required: sn_ot_incident_write

About this task
Fields that are copied over to the child incident are configured by using the *com.snc.sn_ot_incident.copy.attributes* system property.

Procedure

1. Navigate to the **OT Incidents** list module in the Industrial Workspace.
   Alternatively, you can go to an OT device record or equipment model entity record and select the **OT Incidents** tab.
2. Open the OT incident that you want to create a child incident for.
3. Select the **Child Incidents** related list.
4. Select **New**.
5. Fill in the details of the child incident.
6. Select **Save**.

Result
Now, you can view and edit the child incident in the parent incident record.

Visibility of incidents across sites

With the Operational Technology (OT) incident fulfiller role (sn_ot_incident_write), you can view, create, or edit the incidents that belong to your site. You can also view the incidents that belong to other sites to help resolve similar incidents at your site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT incident visibility overview

If you're a user with the OT incident fulfiller role (sn_ot_incident_write), you can do the following tasks:

- View and edit the OT incident records that are assigned to you or the incidents that belong to your site.
- Create OT incidents.
- View OT incidents that belong to the other sites.

Benefit of the OT incident fulfiller role

The main benefit of being an OT incident fulfiller is that you have read-only visibility of incidents across sites. Viewing other incidents across sites can help you resolve similar incidents at your site.

Note: You can't edit OT incidents for other sites. You can only edit incidents that belong to your site.

Where to view or edit incidents

The following OT incident lists are available in the Lists module on the Industrial Workspace:

- Assigned to me: View and edit your assigned incident records by navigating to **OT Incidents** > **Assigned to me**.
- Belong to my sites: View and edit the incident records that belong to your sites by navigating to **OT Incidents** > **Belong to my sites**.
- View the existing incident records at different sites by navigating to **OT Incidents** > **All**.

Synchronization between an incident and its incident tasks

You can use Operational Technology (OT) incident tasks to collaborate with and request work from other stakeholders. An OT incident and its tasks are synchronized so that the state of the incident tasks change depending on the state of incident.

The *com.snc.incident.ot_incident_task.closure* property closes open incident tasks when the related incident is closed or canceled. This property is responsible for different actions that take place on OT incident tasks based on the state of the OT incident.

The synchronization between an OT incident and its open OT incident task is as follows:

- When an OT incident is closed, the state of any open OT incident task is set to **Closed Incomplete**.
- When an OT incident is canceled, the state of any open OT incident task is set to **Closed Skipped**.

Incident email notifications

Use Operational Technology (OT) incident email notifications to alert users when changes are made to an incident.

The notifications are listed in the following table.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT incident email notifications

Notification name	When to send	Who receives it	What it contains
Incident commented	When an extra comment is added	Assigned to, Watch list	Subject: <Incident #> - comment added Body: Comment added URL to the incident
Incident opened and unassigned	When the **Assigned to** field changes to empty and **Active** is true	The one who opened the incident	Subject: <Incident #> - is unassigned Body: Please identify someone to work on this incident URL to the incident
Incident closed	When the incident is closed	Assignment group	Subject: <Incident #> - is closed Body: Resolution Code and Resolution Notes
Incident priority changed	When triggered	Assigned to, Assignment group, Watch list	Subject: <Incident #> - priority changed Body: New priority: <priority>
Incident resolved	When the incident state changes to **Resolved**	Caller, Watch list	Subject: <Incident #> - is resolved Body: Resolution Code and Resolution Notes
Incident assigned to my group	When the **Assignment Group** field changes	Assignment group, Watch list	Subject: <Incident #> - is assigned to <assignment group> Body: Priority, Short description, Description URL to the incident
Incident assigned to me	When the **Assigned to** field changes	Assigned to, Watch list	Subject: <Incident #> - is assigned to you

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT incident email notifications (continued)

Notification name	When to send	Who receives it	What it contains
			Body: Priority, Short description, Description URL to the incident
Incident opened for me	When a new incident is created	Caller	Subject: <Incident #> - is opened on your request Body: Priority, Short description, Description URL to the incident
Incident state changed	When the state of the incident changes	Assigned to, Watch list	Subject: <Incident #> - State changed Body: Short description, Old State, New State URL to the incident

Compose an email from an OT incident record

Compose an email directly in an OT incident record so that you can conveniently update your team and others about the incident.

Before you begin

Role required: sn_ot_incident_write

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the OT Incidents list module, select one of the available lists.
4. Select the incident record that you want to send an email for.
5. In the incident header, open the menu by selecting the **More actions** ... button.
6. Select **Compose Email**.
7. On the email template, fill in the form.

Email template form

Field	Description
To	User or users that you want to send the email to.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	This field automatically fills in the user in the **Assigned to** field of the OT incident record.
Subject	Subject of the email. This field automatically fills in the number of the OT incident record and its short description.
Body	Updates that you want to send to a user or users that are related to the OT incident.

8. **Optional:** If the email is a response, you can use a response template in the **Response Templates** field to fill in the email body.
9. **Optional:** To save the email as a draft, select **Save as draft**.
10. Select **Send Email**.

Result
The email is sent to the user or users that you specified in the email template.

Resolve and close an incident

When an issue is corrected, you can set the Operational Technology (OT) incident state to **Resolved**. If you're happy with the resolution, you can close the incident. The incident also auto-closes after a certain amount of time based on the incident auto-close properties.

Before you begin
Role required: sn_ot_incident_write

Procedure
1. Navigate to **All** > **Incident** > **Open**.
2. Open the in-progress OT incident that you want to resolve and close.
3. In the **Resolution Information** related list, fill in the following fields.

Resolution Information fields

Field	Description
Resolution code	Information to categorize resolved cases. **Duplicate** Incident is a duplicate of an existing incident and should be closed. **Known error** Incident was resolved by a solution from a known error. **Resolved by caller** Incident was resolved by the user who contacted the OT engineer for the issue.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
	Resolved by change Incident was resolved with an OT change request. For more information about OT change requests, see Create a change request. **Resolved by problem** Incident was resolved with a problem that identified the cause of the incident. For more information about problems, see Managing Problems. **Resolved by request** Incident was resolved by an OT request. For more information about OT requests, see Create an Operational Technology request on the Industrial Workspace. **Solution provided** Solution for the incident was provided that doesn't fit the other resolution codes.
Resolution notes	Describes how the incident was resolved.

4. In the **State** field, select **Resolved**.
5. Click **Update**.

Edit the related devices and equipment model entities in an incident record

Add or remove the related Operational Technology (OT) devices and equipment model entities directly from an OT incident record. You can track the relationship between the incident and its affected items.

Before you begin

Role required: sn_ot_incident_write or sn_ot_incident_admin

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the OT Incidents list module, select one of the available lists.
4. Select the incident record that you want to edit.
5. Add or remove a related OT device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Action	Description
Add a related OT device from the incident record	**a.** Select the Affected OT Devices related list. **b.** Select **Add**. **c.** In the Add OT Devices window, select the check boxes next to the devices that you want to add. **d.** Select **Add**.
Remove a related OT device from the inci dent record	**a.** Select the Affected OT Devices related list. **b.** Select the check boxes next to the devices that you want to remove. **c.** Select the **Remove** button. **d.** In the confirmation window that appears, se lect **Remove**.

The OT devices are now added to or removed from the change record in the Affected OT Devices related list.

6. Add or remove an equipment model entity from an incident record by repeating steps 4 and 5 but in the Impacted Equipment Model Entities related list.

Operational Technology Incident Management reference

Reference topics provide additional information about the Operational Technology Incident Management application.

Assignment rule form

Assignment rules automatically assign an Operational Technology (OT) incident to a group or user according to one or more conditions in the assignment rule.

The following table describes the field values for the Assignment rule form.

Assignment rule form

Field	Description
Name	Descriptive name for the assignment rule.
Active	Option to activate the assignment rule.
Applies to	
Table	Table with the records that the assignment rule applies to. **Note:** For assignment rules that are specific to OT incidents, set the Table field to **Operational Technology Incident [sn_ot_incident]**. The list shows only the tables and database views that are in the same scope as the assignment rule. If you select a custom table that extends the task table and to make sure that the assignment rule works properly, you must clear the instance cache by navigating to https://<instance_name>.service-now.com/cache.do.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assignment rule form (continued)

Field	Description
	Important: Clearing the system cache can affect the overall performance and may degrade the system response times. Don't run cache flushes during business hours, and don't trigger cache flushes to run automatically.
Conditions	Conditions under which the assignment rule applies.
Assign to	
User	User that the event is assigned to.
Group	Group that the event is assigned to.
Script	
Script	Script to specify the advanced assignment rule functionality. The current.variable_pool set of variables is available. **Note:** Make sure that the input in the script is correct and that the input type matches the field type in the Assignment Rule script. For example, if the assignment rule script sets the value of an Integer field, and the value in the script is set to String, the assignment rule may yield unexpected results.
Optional fields	
Match conditions	**Any** If any of the conditions are met, the assignment rule applies. **All** If all the conditions are met, the assignment rule applies.
Execution Order	Order in which the assignment rule is processed. If the assignment rules conflict, a rule with a lower-order value takes precedence over a rule with a higher value. If the order values are set to the same number, the assignment rule with the first matching condition takes precedence over the others without the first matching condition. Only the first assignment rule with a matching condition runs against a record.

Components installed with Operational Technology Incident Management

Several types of components may be installed with activation of the Operational Technology Incident Management (sn_ot_inc_mgmt) plugin, including user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Roles installed

Role	Description	Contains roles
OT Incident Admin [sn_ot_incident_admin]	Can create, view, delete and edit OT incident records for any equipment model entities. Can configure **Priority Lookup Rules** and **OT incident system properties**.	• cmdb_ot_isa_viewer_all • sn_ot_incident_write

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Role	Description	Contains roles
OT Incident Reader [sn_ot_incident_read]	Can only view OT incident records.	• cmdb_ot_viewer • cmdb_ot_isa_viewer
OT Incident Fulfiller [sn_ot_incident_write]	Can view, create, and edit OT incident records.	sn_ot_incident_read

Note: The OT Incident User [ot_incident_user] role is deprecated. For users assigned this role, you can execute a scheduled job to assign them new Operational Technology Incident Management roles. For more information, see Assign new roles to your users.

Tables installed

Table	Description
OT Incidents [sn_ot_incident]	List of OT incidents reported across sites.
OT Incident Tasks [sn_ot_incident_task]	List of OT incident tasks created under various OT incidents.
OT Incident Priority Rule Lookup [dl_ot_inc_priority]	List of rules to calculate the priority of an OT incident.

Related information

Find more information about the OT extension classes and related applications.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Operational Technology (OT) extension classes

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

IT Service Management

When integrated with Operational Technology Incident Management, the ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Operational Technology Change Management

The ServiceNow® Operational Technology Change Management application enables your organization to implement changes to Operational Technology (OT) devices and production processes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Explore	Configure
 Exploring Operational Technology Change Management	 Plan and configure your implementation
Use	**Reference**
 Using Operational Technology Change Management	 Get details about related information and applications

Exploring Operational Technology Change Management

Learn more about the Operational Technology Change Management application.

Operational Technology Change Management overview

Watch an overview about the Operational Technology Service Management product suite to learn more about the Operational Technology Change Management application.
https://player.vimeo.com/video/1019801515?badge=0&autopause=0&player_id=0&app_id=58479

Key features

With the Operational Technology Change Management application, you can use the following key features:

- Digitized change workflow that connects all stakeholders.
- Sites that have different change management processes (workflows).
- Separated IT Change Management and Operational Technology Change Management, but ability to be combined if necessary.
- Integrated Operational Technology Change Management workflow with the Operational Technology Incident Management and Operational Technology Vulnerability Response applications.
- Aligned factory floor changes for the equipment model entities with downtime schedules.

Using Operational Technology Change Management to optimize your production process

The Operational Technology Change Management application enables your team members to work collaboratively on changes to Operational Technology (OT) devices or industrial equipment

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

configurations. These changes include any optimizations, alterations in the production process, or vulnerability fixes.

Operational Technology Change Management overview

By using the Operational Technology Change Management application, you can manage your OT change requests separately from your Information Technology (IT) change requests. You can separate OT change requests from IT change requests by the network type and you can manage OT change requests per site.

The following examples show how to apply Operational Technology Change Management to your organization:

- An OT remediation owner, who's responsible for fixing vulnerabilities on OT devices, wants to initiate a change to fix a group of vulnerabilities.
- An OT technician, who's responsible for OT configurations and plant engineering activities, wants to execute a change to fix a malfunctioned robotic arm on the industrial floor.
- A plant head, who's responsible for overall production activity, wants to review and approve a change requested by the engineering team.

OT change requests

OT change requests occur when there's a disruption in service from an OT device on an OT network. In some cases, the OT device may not be known when the change request is created. When you create an OT change request from the Industrial Workspace, the change request is automatically assigned a Network Type of **OT**. This attribute is used to distinguish an OT change request from an IT change request. This field isn't displayed by default. For more information about OT devices, see OT device related items and related lists.

For more information about how to create an OT change request, see Create a change request.

Separating an IT and OT change

When the Operational Technology Change Management application is installed on your instance, you can choose a Network Type of **IT**, **OT**, or **None**. New change requests are assigned a Network Type of **None** by default.

Operational Technology Change Management model state transitions

The following tables list the Operational Technology Change Management model state transitions for both the Basic OT Change Model and the Advanced OT Change Model. For more information about the OT Change Models, see Select a change model to fulfill change requests.

States for the Basic OT Change Model

State	Description
New	An OT change request is initiated.
Plan	The OT change request is analyzed with the following criteria: • Justification • Implementation plan • Risk and impact analysis • Backout plan

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

States for the Basic OT Change Model (continued)

State	Description
	• Test plan • Schedule the change
Implementation	The change is performed on the targeted OT device.
Closed	The change record is closed after the change is completed.
Canceled	The change record is canceled and the change isn't applied to the OT device.

States for the Advanced OT Change Model

State	Description
New	An OT change request is initiated.
Plan	The OT change request is analyzed with the following criteria: • Justification • Implementation plan • Risk and impact analysis • Backout plan • Test plan • Schedule the change
Approve	The reviewers approve or deny the OT change request.
Implementation	The change is performed on the targeted OT device.
Post-Implementation Review	Add additional OT change tasks if needed and perform the following checks: • Electrical check • Network check • Quality check • Safety check
Closed	The change record is closed after the change is completed.
Canceled	The change record is canceled and the change isn't applied to the OT device.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuring Operational Technology Change Management

Configure the Operational Technology Change Management application so that you can create the data foundation for the ServiceNow® Operational Technology (OT) solution.

If you have the admin role, you can use the Guided Setup to lead you through the setup of the Operational Technology Change Management application. Guided Setup is a tool that assists with application configuration. It organizes the configuration activities into categories. These categories contain the information about the setup tasks, steps to complete each task, and links to the pages in your instance where you perform the configuration. Links to useful help content are also provided.

Note:

Operational Technology Change Management is dependent on Utah P4 or later releases.

To access the Guided Setup, navigate to *Industrial Workspace Admin* > **Guided Setup**.

The following table explains the Guided Setup tasks and their purpose for the Operational Technology Change Management application.

Task	Purpose
1. Install the Operational Technology Change Management application from the ServiceNow Store.	Installs the Operational Technology Change Management application and supporting plugins.
2. Assign Operational Technology Change Management roles.	Assigns the roles to control the actions that are available for each user.
3. Configure Operational Technology Change Management categories.	Configures the categories for the OT changes that are needed for your organization.
4. Select the Operational Technology Change Management model.	Selects the change model for your organization.

Install Operational Technology Change Management

You can install the Operational Technology Change Management application (sn_ot_chg_mgmt) if you have the admin role.

Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- The Operational Technology Change Management application requires the following plugins. Ensure that these plugins are activated before you install the Operational Technology Change Management application.

  Required ServiceNow plugins

  CMDB CI Class Models (sn_cmdb_ci_class)

  The Configuration Management Database (CMDB) CI Class Models store app adds class models that extend the CMDB class hierarchy, including the class descriptions, identification rules, identifier entries, and dependent relationships. For more information, see CMDB CI Class Models store app.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

ISA Equipment Model (sn_isa_model)

The data model for ISA-95 equipment model entities and templates. For more information, see ISA-95 equipment model.

- The Operational Technology Change Management application requires either one or both of the following ServiceNow Store applications. Ensure that at least one of these applications is installed before you install the Operational Technology Change Management application.

  Required ServiceNow Store applications

  Operational Technology Manager

  The Operational Technology Manager application creates the foundational data and relationships that enable your organization to use the Operational Technology solution. The Operational Technology Manager application supports the use of the Configuration Management Database (CMDB), Service Graph Connectors, and Discovery applications in the ServiceNow AI Platform. For more information, see Configuring the Operational Technology Manager.

  Industrial Process Manager

  The Industrial Process Manager application creates the ISA-95 Equipment Model data foundation that is required for the ServiceNow® Industrial solution, enabling you to create your own version of the equipment models in each of your industrial sites. For more information, see Configure the Industrial Process Manager.

Role required: admin

About this task

The following items are installed with the Operational Technology Change Management application:

- Plugins
- Store applications
- Roles and ACLs

For more information about the roles and ACLs installed, see Components installed with Operational Technology Change Management.

Note: For Operational Technology Service Management users with no license for Operational Technology Visibility, note the following:

- When you have the latest version of Operational Technology Incident Management installed, Industrial Process Manager is also installed.
- When you have the latest version of Operational Technology Change Management installed, Industrial Process Manager is also installed.

You should upgrade to the latest versions so you have access to the Operational Technology Service Management experience.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the Operational Technology Change Management application by using the filter criteria and search bar.

   You can search for the application by its name or ID. If you can't find the application, you might have to request it from the ServiceNow Store.

   Visit the ServiceNow Store to view all the available apps, and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.
3. In the Application installation dialog box, review the application dependencies.

   Dependent plugins and applications are listed if they'll be installed, are currently installed, or must be installed. If any plugins or applications must be installed, you must install them before you can install the Operational Technology Change Management application.
4. Select **Install**.

Assign Operational Technology Change Management roles

Assign roles to your users so that you can control their access to the features, capabilities, and data in the Operational Technology Change Management application.

Before you begin

Role required: admin or user_admin

About this task

Users with the roles that are listed in the following table can use the application.

Role	Description
Change Manager [sn_ot_change_manager]	Can manage OT change model records.
Change Admin [sn_ot_change_admin]	Can create, view, delete, and edit OT change records. Can configure categories and system properties.
Change Write user [sn_ot_change_write]	Can create, view, and edit OT change records. Can also be assigned IT change tasks, and can edit and close the IT change task they're assigned to. For more information, see Managing change requests across sites.
Change Read user [sn_ot_change_read]	Can only view OT change records.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Select a change model to fulfill change requests

Select an Operational Technology (OT) change model to begin fulfilling your change requests depending on the needs of your organization.

Before you begin

Role required: sn_ot_change_admin or admin

About this task

Two OT change models are available for you to use:

- OT Change Basic
- OT Change Advanced

The OT Change Basic model uses the change process without approvals.

For more information about the OT Change Basic Model, see Basic OT Change Model playbook.

The OT Change Advanced model uses the change process with approvals. You can create a change approval policy and assign an approval group to review your change request. For more information about change approvals, see Operational Technology change approval.

For more information about the Advanced OT Change Model, see Advanced OT Change Model playbook.

Procedure

1. Navigate to **Industrial Workspace Admin** > **Guided Setup**.
2. In the Operational Technology Change Management category, select **Get Started**.
3. Next to the Change Models section, select **Configure**.
4. Select the change model that fits the needs of your organization.
5. Edit the record as needed.

Result

The change model is applied to your system and you can begin creating OT change requests.

Basic OT Change Model playbook

Learn about the Basic Operational Technology (OT) Change Model playbook stages that an OT change without approvals must go through until it's completed.

Initiate

The Initiate stage of an OT change request lets you capture the details of the requested change and assign the change as necessary. This stage has three tasks.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Describe the change

Field	Description
Short description	Brief description of the change.
Description	Details of the change.
Category	Type of change.
Site	Site where the change takes place.
Watch list	Users who receive notifications about this change when comments are added.
Work notes list	Users who receive notifications about this change when work notes are added.

Capture risk

Field	Description
Priority	Impact and urgency to identify how quickly the change should be addressed.
Risk	Amount of risk that the change poses.
Impact	Measure of the effect that a change has on your industrial processes.

Assign the change

Field	Description
Requested by	User who requests the change.
Assignment group	Assigned group that works on the change. The assignment group can be any group with the type OT.
Assigned to	User who works on this change. If the assignment group changes, the **Assigned to** field is cleared.

Plan

The Plan stage of an OT Change request lets you add a justification for the change, an implementation plan, a risk and impact plan, a backout plan, a test plan, and a time to schedule the change. This stage has six tasks.

Add a justification

Field	Description
Justification	Reason why the change must take place.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add implementation plan

Field	Description
Implementation plan	Details of how to implement the requested change.

Add risk and impact analysis

Field	Description
Risk and impact analysis	Details of any risk and impact factors that are related to this change.

Add backout plan

Field	Description
Backout plan	Details of how to reverse the change in place if necessary.

Add test plan

Field	Description
Test plan	Details of how to test the implemented change.

Schedule the change

Field	Description
Planned start date	Date that the change takes place. **Note:** You can also choose an available downtime slot on the calendar by selecting the **Scheduling Assistant** button to fill in the planned start date field automatically.
Planned end date	Date that the change ends. **Note:** You can also choose an available downtime slot on the calendar by selecting the **Scheduling Assistant** button to fill in the planned end date field automatically.

Implement

The Implement stage of an OT change request provides the details of the following task. You can mark this stage as complete when it's finished.

Perform the change

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mark as complete when the change is performed on the targeted OT devices and completed.

Close

The Close stage lets you close the change record after the change is completed.

Close the change record

Field	Description
Close code	Reason that the change record was closed.
Close notes	Additional details about closing the change record.

Advanced OT Change Model playbook

Learn about the Advanced Operational Technology (OT) Change Model playbook stages that an OT change with approvals must go through until it's completed.

Initiate

The Initiate stage of an OT Change request lets you capture the details of the requested change and assign the change as necessary. This stage has three tasks.

Describe the change

Field	Description
Short description	Brief description of the change.
Description	Details of the change.
Category	Type of change.
Site	Site where the change takes place.
Watch list	Users who receive notifications about this change when comments are added.
Work notes list	Users who receive notifications about this change when work notes are added.

Capture risk

Field	Description
Priority	Impact and urgency to identify how quickly the change should be addressed.
Risk	Amount of risk the change poses.
Impact	Measure of the effect that a change has on your industrial processes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign the change

Field	Description
Requested by	User who requests the change.
Assignment group	Assigned group that works on the change. The assignment group can be any group with the type OT.
Assigned to	User who works on this change. If the assignment group changes, the **Assigned to** field is cleared.

Plan

The Plan stage of an OT change request lets you add a justification for the change, an implementation plan, a risk and impact plan, a backout plan, a test plan, and a time to schedule the change. This stage has six tasks.

Add justification

Field	Description
Justification	Reason why the change must take place.

Add implementation plan

Field	Description
Implementation plan	Details of how to implement the requested change.

Add risk and impact analysis

Field	Description
Risk and impact analysis	Details of any risk and impact factors that are related to this change.

Add backout plan

Field	Description
Backout plan	Details of how to reverse the change in place if necessary.

Add test plan

Field	Description
Test plan	Details of how to test the implemented change.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Schedule the change

Field	Description
Planned start date	Date that the change takes place. **Note:** You can also choose an available downtime slot on the calendar by selecting the **Scheduling Assistant** button to fill in the planned start date field automatically.
Planned end date	Date that the change ends. **Note:** You can also choose an available downtime slot on the calendar by selecting the **Scheduling Assistant** button to fill in the planned end date field automatically.

Approve

The Approve stage of an OT Change request lets reviewers approve or deny the OT Change. This stage includes only one task.

Review and take action

Field	Description
Approve button	If you're a reviewer shown in the table on the task form, select **Approve** to accept the change.
Deny button	If you're a reviewer shown in the table on the task form, select **Deny** to reject the change.
Comments	Additional information about the approval or denial of the change.

For more information about change approvals, see Operational Technology change approval.

Implement

The Implement stage of an OT change request provides the details of the following tasks. You can mark this stage as complete when it's finished.

Stop the function

If needed, mark as complete after you stop the function of the targeted OT devices.

Ensure LOTO

Lockout/Target (LOTO) is a safety procedure to prevent accidental or unintentional start-up of machinery during maintenance or service. Mark as complete when LOTO is completed.

Perform the change

Mark as complete when the change is performed on the targeted OT devices and completed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Post-implementation Review

The Post-implementation Review stage of an OT change request lets you check off the performed tasks, create additional OT change tasks for remaining work identified during the review, and mark the revoke LOTO process as complete.

Perform checks

Field	Description
Perform electrical check	Check box that you select after the electrical check has been completed.
Perform network check	Check box that you select after the network check has been completed.
Perform quality check	Check box that you select after the quality check has been completed.
Perform safety check	Check box that you select after the safety check has been completed.

Recommend spin-off tasks

Field	Description
OT Change Tasks	List of the change tasks that are related to the OT change.
State	State of the OT change. The state moves and tracks changes through several stages of resolution.
Assigned to	User who works on this change. If the assignment group changes, the **Assigned to** field is cleared.
Short description	Brief description of the change task.

Revoke LOTO

After the change is implemented and reviewed, mark as complete when the lockout-target is revoked.

Spin-off Tasks

The Spin-off Tasks stage lists all the change tasks in the Post Implementation Review that must be completed.

Close

The Close stage lets you close the change record after the change is completed.

Close change record

Field	Description
Close code	Reason that the change record was closed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Close change record (continued)

Field	Description
Close notes	Additional details about closing the change record.

Using Operational Technology Change Management

After you complete all required set-up tasks for the Operational Technology Change Management application, you can begin managing Operational Technology (OT) change requests.

Create a change request

Create an Operational Technology (OT) change request to report a change in your site.

Before you begin

Role required: sn_ot_change_write

About this task

For a walkthrough of how to create an OT change request, watch this video.

https://player.vimeo.com/video/1154461579?h=42cc370e20&badge=0&autopause=0&player_id=0&app_id=58479

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the **OT Change Requests** list view, select the list you want to open.
3. Select **New**.
4. Select the OT change model that applies to your organization.
5. Select **Create OT Change Record**.
6. Complete the playbook as needed as your team works on the change request.
   For more information about the Basic OT Change Model playbook, see Basic OT Change Model playbook. For more information about the Advanced OT Change Model playbook, see Advanced OT Change Model playbook.

   Note: If you don't have Playbook enabled, you can only view the **Details** and **Related Records** tabs in the OT change request record.

Create a change task to fulfill a change request

Create a change task to fulfill an Operational Technology (OT) change request. Change tasks help to capture all the tasks that need to take place during a change request.

Before you begin

Role required: sn_ot_change_write

About this task

Change tasks are the individual steps that must take place to fulfill and complete a change request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the change record that you want to create a task for.
3. In the Change Tasks related list, select **New**.
   If you don't see the Change Tasks related list, you must add it.
4. On the form, fill in the fields.

Incident task form

Field	Description
OT Change Task	
Short description	Brief description of the change task.
Description	Details of the change task.
OT device	Affected OT device.
OT change request	Record number of the related OT change request.
State	State for tracking a change task through several stages of the change implementation.
Type	Type of change.
Assignment	
Assignment group	Group who works on the change task. If you leave this field empty, the change task is automatically assigned.
Assigned to	User to whom the change task is assigned to work on. **Note:** If the **Assignment group** changes, the **Assigned to** field is cleared.
Notes	
Watch list	Users who receive notifications about this change when comments are added.
Work notes list	Users who receive notifications about this change when work notes are added.
Work notes (Private)	Work notes that aren't available to customers.

5. Select **Save**.

Result

You can view and edit the change task in the related OT change record.

You can view change tasks in the Industrial Workspace list view in the following places.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Change tasks assigned to you: **OT Tasks** > **Assigned to Me**
- Change tasks assigned to your group: **OT Tasks** > **Assigned to My Groups**
- Unassigned change tasks: **OT Tasks** > **Unassigned**

Create a change request from OT device details

Create an Operational Technology (OT) change request from an OT device record. Creating a change request from a device record automatically populates the information in your change request record, such as the site or business service and the OT Device field.

Before you begin

Role required: sn_ot_change_write

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the All OT Devices list, select an OT device record.
3. Under the **Related Records** tab, select the OT Change Requests related list.
4. Select **New**.
5. Select the OT change model that applies to your organization.
6. Select **Create OT Change Record**.
7. Complete the playbook as needed as your team works on the change request.

   For more information about the Basic OT Change Model playbook, see Basic OT Change Model playbook. For more information about the Advanced OT Change Model playbook, see Advanced OT Change Model playbook.

   The following fields are automatically populated depending on the conditions that you set.

   - The **OT Device** field is auto-populated only if the Industrial Process Manager application is enabled.
   - If the Industrial Process Manager is installed, then the site assigned to the OT device shows up in the **Site** field.
   - If the Industrial Process Manager is enabled and there's only one entity that is associated with the OT device, then the **Equipment model entity** field is automatically populated.

     Note: If multiple entities are associated with an device, the **Equipment model entity** field is left empty.

Result

The change request is created, and the users in the Assignment group, Assigned to, and Watch list fields are notified.

Create a change request from a remediation task

Create an Operational Technology (OT) change request from an OT remediation task. Creating a change request from a remediation task automatically populates the information in your change request record, such as the Site and the OT Device fields.

Before you begin

Roles required: sn_ot_change_write or sn_otvr.remediation_owner

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the remediation task record that you want to create a change request from.
3. Select the **Create OT Change** button.

   Note: If there's no active change model, the following error appears: `Error creating Change Request: No active change model available. Please contact your OT Change admin.`

4. Select the OT change model that applies to your organization.
5. Select **Next**.
6. Complete the playbook as needed as your team works on the change request.

   For more information about the Basic OT Change Model playbook, see Basic OT Change Model playbook. For more information about the Advanced OT Change Model playbook, see Advanced OT Change Model playbook.

   The following fields are automatically populated depending on the conditions that you set.

   - The **OT Device** field is auto-populated only if the Industrial Process Manager application is enabled.
   - If the Industrial Process Manager is installed, then the site assigned to the OT device shows up in the **Site** field.
   - If the Industrial Process Manager is enabled and there's only one entity that is associated with the OT device, then the **Equipment model entity** field is automatically populated.

     Note: If multiple entities are associated with an device, the **Equipment model entity** field is left empty.

Create a change request from an incident record

Create an Operational Technology (OT) change request from an OT incident record. By creating a change request directly from an incident record, the data is automatically mapped to the new change request from the incident record.

Before you begin

Role required: sn_ot_incident_write, sn_ot_incident_admin, or sn_ot_change_write

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the OT Incidents list module, select one of the available lists.
3. Select the incident record that you want to create an OT change request from.
4. Select the **Create OT Change** button.
   The Select OT change form opens.
5. Select the change model that is applicable to your organization.
   For more information, see Select a change model to fulfill change requests.
6. Select **Create OT Change record**.
7. Fill in the playbook and related forms as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about the playbook and related forms, see Basic OT Change Model playbook and Advanced OT Change Model playbook depending on which OT change model you chose.

Note: In the Details related list of the new change request, the following fields and related lists are automatically filled in with the values from the related OT incident record:

- Site
- Equipment Model Entity
- OT Device (CI)
- Short Description
- Description
- Priority

  Note: A **Priority** field value from 1 through 4 is the same in the new change record. But a value of 5 in the incident record's **Priority** field is changed to 4 in the new change record.

Edit the related devices and equipment model entities in a change record

Add or remove the related Operational Technology (OT) devices and equipment model entities directly from an OT change record. You can track the relationship between the change request and its affected items.

Before you begin

Role required: sn_ot_change_write or sn_ot_change_admin

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the OT Change Requests list module, select one of the available lists.
4. Select the change record that you want to edit.
5. Add or remove a related OT device.

Action	Description
Add a related OT device from the change record	**a.** Select the Affected OT Devices related list. **b.** Select **Add**. **c.** In the Add OT Devices window, select the check boxes next to the devices that you want to add. **d.** Select **Add**.
Remove a related OT device from the change record	**a.** Select the Affected OT Devices related list. **b.** Select the check boxes next to the devices that you want to remove. **c.** Select the **Remove** button. **d.** In the confirmation window that appears, se lect **Remove**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The OT devices are now added to or removed from the change record in the Affected OT Devices related list.

6. Add or remove an equipment model entity from a change record by repeating steps 4 and 5 but in the Impacted Equipment Model Entities related list.

Operational Technology change approval

The Operational Technology (OT) change approval lets reviewers approve your requested changes and suggest improvements as necessary.

Change approval overview

An OT change approval with the Advanced OT Change Model enables approvers to review a change request, edit the request as necessary, and approve the change request.

Note: The change approval only applies to the Advanced OT Change Model. There's no change approval policy applied to the Basic OT Change Model.

Change approval requirements

Requirement	Description
Site level	Site or area where the change takes place.
Site approval group	Members assigned to an approval group that can review and approve change requests.
Role required	Approvers must have the sn_ot_change_read role.
Percentage of approvals	51% of the approval group has to approve the change for it to move forward.

OT change approval flow

The OT change approval flow is as follows.

1. Create the change request.
2. The flow is invoked based on the change model.
3. The flow applies the change approval policy.
4. Various decision records are evaluated.
5. Matching approval definitions are executed.
6. Add a list of site level approvers to the change record.

The Advanced OT Change Model contains a change approval policy. You can also create your own approval policy. For more information about how to create an approval policy, see Create change approval policies.

Add an approver to review a change request

Add a group member, or approver, manually to your approval group to review your Operational Technology (OT) change request.

Before you begin
Role required: admin

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **User Administration** > **Groups**.
2. From the Groups list, select the **OT Change Default Approvers** group.
3. Select the Group Members related list.
4. Select **Edit**.
5. In the Collection list, select the members that you want to add to the approval group.
6. Move the selected members to the OT Change Default Approvers list by using the middle arrows.
7. Select **Save**.

Result

New members have been added to your approval group. Now, the approval group can review your change request.

Once you complete the Initiate and Plan stages of your OT change request in the Advanced OT Change Model playbook, you can request an approval in the Approve stage. The member or members in your approval group must open the change request record to approve it in the Industrial Workspace using either of the following methods.

- In the change request record, select the **Approvers** tab and change the **State** field from **Requested** to the appropriate option.
- In the **Playbook** tab, select the Approve stage and change the **State** field from **Requested** to the appropriate option.

Managing change requests across sites

You can view, create, or edit the change requests that belong to your site or other sites by using the Operational Technology Change Management application. By viewing the change requests from other sites, you can implement similar changes at your site.

Change requests across sites overview

If you have the sn_ot_change_write role, you can do the following tasks:

- View and edit the Operational Technology (OT) change requests that are assigned to you or the change requests that belong to your site.
- Create the OT change requests.
- View the OT change requests that belong to the other sites.

The main benefit of having the sn_ot_change_write role is that you have read-only visibility of changes across sites. Viewing other changes across sites can help you implement similar changes at your site.

Note: You can only edit OT change requests belonging to sites you have access to. Learn more about additional roles required for managing cross-site OT change requests in the following sections.

Other OT roles and permissions that you need with the sn_ot_change_write role

The following table describes the additional roles that you, as a user with the sn_ot_change_write role, need so that you can access the change requests for your site or any site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Other roles that you need with the sn_ot_change_write role

Role	Permissions
sn_ot_change_write with the cmdb_ot_isa_editor role	Create and edit the change requests for your site.
sn_ot_change_write with cmdb_ot_isa_viewer role	Create and edit the change requests for your site.
sn_ot_change_write and cmdb_ot_isa_viewer_all	Create and edit the change requests for any site.
sn_ot_change_write with no site role	View the change requests for any site.

Other OT roles and permissions that you need with the sn_ot_change_read role

The following table describes the additional roles and permissions that you, as a user with the sn_ot_change_read role, need so that you can view the change requests for your site or any site.

Other roles that you need with the sn_ot_change_read user role

Role	Permissions
sn_ot_change_read with the cmdb_ot_isa_editor role	View the change requests for your site.
sn_ot_change_read with cmdb_ot_isa_viewer role	View the change requests for your site.
sn_ot_change_read and cmdb_ot_isa_viewer_all	View the change requests for any site.
sn_ot_change_read with no site role	View the change requests for any site.

Where to view or edit change requests

The following OT change request lists are available in the Lists module on the Industrial Workspace:

- Assigned to me: View and edit your assigned change records by navigating to **OT Change Requests** > **Assigned to me**.
- Belong to my sites: View and edit the change records that belong to your sites by navigating to **OT Change Requests** > **Belong to my sites**.
- View the existing change records at different sites by navigating to **OT Change Requests** > **All**.

Visibility of change model records across sites

Depending on your Operational Technology (OT) change role and site role, you can view, create, or edit the change model record for your site or other sites.

OT Change roles and visibility to change model records

The following tables describe the roles and permissions for different OT change users to access change model records.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Permissions for users with the sn_ot_change_write role

Role	Permissions
sn_ot_change_write with cmdb_ot_isa_editor site role	Use a change model for their records.
sn_ot_change_write with cmdb_ot_isa_viewer site role	Use a change model for their records.
sn_ot_change_write with cmdb_ot_isa_viewer_all site role	Use a change model for their records.
sn_ot_change_write with no site role	No access to change models.

Permissions for users with the sn_ot_change_read role

Role	Permissions
sn_ot_change_read with cmdb_ot_isa_editor site role	No access to change models.
sn_ot_change_read with cmdb_ot_isa_viewer site role	No access to change models.
sn_ot_change_read with no site role	No access to change models.
sn_ot_change_read with cmdb_ot_isa_viewer_all site role	No access to change models.

Permissions for users with the sn_ot_change_manager role

Role	Permissions
sn_ot_change_manager with cmdb_ot_isa_editor site role	• Create, edit, and delete change models for any site. • Assign change models to any site. • Remove change models from any site.
sn_ot_change_manager with cmdb_ot_isa_viewer site role	• Create, edit, and delete change models for any site. • Assign change models to any site. • Remove change models from any site.
sn_ot_change_manager with no site role	Can’t view or edit change models for any site. Can only view the base system change models that aren't associated with any site.

If you have the sn_ot_change_admin role, you can use the change models to create a change request for any site.

Change email notifications

Use email notifications to alert users when an Operational Technology (OT) change request or a change task is updated.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The notifications for OT change requests and change tasks are listed in the following tables.

OT change request email notifications

Name	When to send	Who receives it	What it contains
Change assigned to me	When the **Assigned to** field changes and is not empty	User who's assigned the change	Subject: <Change request #> notification Body: Short Description: <Short description> Click here to view Change Request: <URL to the change request> Site: <Site name> OT Device: <OT device> Equipment Model Entity: <Equipment model entity> Description: <Description>
Change assigned to my group	When the **Assignment group** field changes and is not empty	Assignment group	Subject: <Change request #> has been assigned to group <assignment group> Body: Short Description: <Short description> Click here to view Change Request: <URL to the change request> Site: <Site name> OT Device: <OT device> Equipment Model Entity: <Equipment model entity> Description: <description>

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT change request email notifications (continued)

Name	When to send	Who receives it	What it contains
Change commented	When the change request is commented	• Requested By • Watch list	Subject: <Change request #> comments added Body: Short description: <Short description> Click here to view Change Request: <URL to the change request> Comments: <Comments added to the change request>
Change worknoted	When a work note is added to the change request.	• Work note list • Assigned to • Assignment group	Subject: <Change request #> work notes added Body: Short description: <Short description> Click here to view Change Request: <URL to change request> Work Notes: <Work notes added to change request>
Change approved	When the change request is approved	• Assigned to • Assignment group	Subject: <Change request #> has been approved Body: Short Description: <Short description> Click here to view <URL to change request> Description: <Description>

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT change request email notifications (continued)

Name	When to send	Who receives it	What it contains
Change rejected	When the change request is rejected	• Assigned to • Assignment group	Subject: <Change request #> has been rejected Body: Short Description: <Short description> Click here to view <URL to change request> Description: <Description>
Change on hold	When the change request is put on hold	Requested By	Subject: <Change request #> has been put on hold Body: Hello <user who created change request>, The <Change request #> you requested has been put on hold. The reason for the request being put on hold is: <Reason for change request being put on hold> Click here to view your change request: <URL to change request>
Change off hold	When the change request is taken off hold	Requested By	Subject: <Change request #> has been taken off hold Body: Hello <user who created change request>, The <Change request #> you requested has been taken off hold and is in the <Updated state field> state.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT change request email notifications (continued)

Name	When to send	Who receives it	What it contains
			Click here to view your change request: <URL to change request>

OT change task email notifications

Name	When to send	Who receives it	What it contains
Change task assigned to me	When the **Assigned to** field changes and is not empty	Person who is assigned the change task	Subject: <Change task #> notification -- <Short description> Body: Short Description: <Short description> Click here to view Change Task: <URL to change task> Site: <Site name> OT Device: <OT device> Equipment Model Entity: <Equipment model entity> Description: <Description>
Change task assigned to my group	When the **Assignment group** field changes and is not empty	Assignment group	Subject: Subject: <Change task #> notification -- <Short description> Body: Short Description: <Short description> Click here to view Change Task: <URL to change task> Site: <Site name> OT Device: <OT device> Equipment Model Entity: <Equipment model entity>

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT change task email notifications (continued)

Name	When to send	Who receives it	What it contains
			Description: <Description>
Change task worknoted	When a work note is added to the change task	• Work note list • Assigned to • Assignment group	Subject: <Change task #> work notes added -- <Short description> Body: Short description: <Short description> Click here to view Change Task: <URL to change task> Work Notes: <Work notes added to change task>

Operational Technology Change Management reference

Reference topics provide additional information about the Operational Technology Change Management application.

Change categories

By categorizing the Operational Technology (OT) change requests, you can group and narrow the search for specific OT change requests. Categories also help stakeholders know what the change is about.

When you can create an OT change request, you can choose from the categories listed in the following table.

Note: You can also configure categories if you have the **admin** or **sn_ot_change_admin** role.

OT change request categories

Category	Description
Hardware	Changes to add, remove, or configure OT devices.
Software	Changes to add, remove, or configure OT software.
Service	Changes to an OT service.
System Software	Changes to the OT system software.
Applications Software	Changes to the OT applications software.
Network	Changes to subnets, IP addresses, and MAC addresses.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT change request categories (continued)

Category	Description
Telecom	Changes to telecommuncations used in your OT system.
Documentation	Changes to the OT documentation.
Firmware	Changes to the OT firmware.
Other	Other changes not captures in the categories above.

Components installed with Operational Technology Change Management

Several types of components may be installed with activation of the Operational Technology Change Management (sn_ot_chg_mgmt) application, including the user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Roles installed

Role	Description	Contains roles
Change Manager [sn_ot_change_manager]	Can manage OT change model records.	• sn_ot_change_write • sn_sttrm_condition_read
Change Admin [sn_ot_change_admin]	Can create, view, delete, and edit OT change records. Can configure categories and system properties.	• cmdb_ot_isa_viewer_all • sn_ot_change_write
Change Write user [sn_ot_change_write]	Can create, view, and edit OT change records. Can also be assigned IT change tasks, and can edit and close the IT change task they're assigned to. For more information, see Managing change requests across sites.	• cmdb_ot_viewer • cmdb_ot_isa_viewer • sn_ot_change_read
Change Read user [sn_ot_change_read]	Can only view OT change records.	• cmdb_ot_viewer • cmdb_ot_isa_viewer

Related information

Find more information about the OT extension classes and related applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Operational Technology (OT) extension classes

The Configuration Management Database (CMDB) updates classes for OT.

Related applications

IT Service Management

When integrated with Operational Technology Change Management, the ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Operational Technology Knowledge Management

ServiceNow® Operational Technology Knowledge Management can help you collect, organize, and share knowledge about your Operational Technology (OT) system, its devices, and the resolved incidents within your organization.

Explore  Exploring Operational Technology Knowledge Management	Configure  Plan and configure your implementation
Use  Using Operational Technology Knowledge Management	Reference  Get details about related information and applications

Exploring Operational Technology Knowledge Management

Operational Technology Knowledge Management helps you to capture information about your Operational Technology (OT) system in knowledge articles that are related to OT incidents. Your organization can then use these knowledge articles to help your users to access the right information and prevent miscommunication with your users.

Operational Technology Knowledge Management overview

Watch an overview about the Operational Technology Service Management product suite to learn more about the Operational Technology Knowledge Management.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

https://player.vimeo.com/video/1019801515?badge=0&autopause=0&player_id=0&app_id=58479

Operational Technology Knowledge Management benefits

With Operational Technology Knowledge Management, you can use the following key features:

- Ability to use the existing Knowledge Management ServiceNow AI Platform capabilities with the Operational Technology Management solution.
- Ability to browse all knowledge base articles that are related to an OT incident and to create knowledge articles directly from an incident record.
- Ability to configure an OT knowledge base for knowledge managers and knowledge users.
- Ability to create knowledge articles in the Industrial Workspace.
- Ability to request approvals to publish, edit, retire, or delete a knowledge article.
- Ability to edit existing knowledge articles with updated information.

Configuring Operational Technology Knowledge Management

Configure Operational Technology Knowledge Management so that you can create the data foundation for the Operational Technology (OT) solution.

If you have the admin role, you can use Guided Setup to lead you through the setup of Operational Technology Knowledge Management. Guided Setup is a tool that assists with application configuration. It organizes the configuration activities into categories. These categories contain the information about the setup tasks, steps to complete each task, and links to the pages in your instance where you perform the configuration. The links to useful help content are also provided.

To access Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

The following table lists the Guided Setup tasks and their purposes for Operational Technology Knowledge Management.

Note: Operational Technology Knowledge Management is included with the Operational Technology Incident Management application. As long as you have the Operational Technology Incident Management application (version 2.0.2) installed and configured, you can configure Operational Technology Knowledge Management. No additional plugins are needed.

The following table shows the tasks that your users must complete for a successful setup and configuration.

Operational Technology Knowledge Management setup tasks

Task	Purpose
Assign Knowledge Management roles to Operational Technology Knowledge Management.	Assigns the roles to control the actions that are available for each user.
Create an OT knowledge base.	Configures an OT knowledge base to add managers and configure access.
Create user criteria to apply to an OT knowledge base.	Creates a user criteria record to determine the users who can read or contribute to an OT knowledge base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Knowledge Management setup tasks (continued)

Task	Purpose
Assign user criteria to an OT knowledge base.	Assigns the user criteria records to an OT knowledge base to control which users can create, read, write, and retire knowledge articles within the knowledge base.
Configure access to OT knowledge bases for unauthenticated users.	Reviews the OT knowledge bases that are accessible to unauthenticated users. Access is based on the user criteria and glide.knowman.block_access_with_no_user_criteria property settings.
Assign knowledge workflows to an OT knowledge base.	Assigns different knowledge workflows to each OT knowledge base for the publishing and retiring processes.
Review the Knowledge Management properties that are used for Operational Technology Knowledge Management.	Configures the look and functionalities of OT knowledge bases with the applicable Knowledge Management properties.

Assign roles to your Operational Technology Knowledge Management users

Assign Knowledge Management roles to your users so that you can control their access to the features, capabilities, and data for Operational Technology Knowledge Management.

Before you begin

Role required: admin

About this task

If you're assigned a Knowledge Management role, you can use the Operational Technology Knowledge Management capabilities.

Note: The user criteria determine the access to knowledge articles. For more information, see Managing access to knowledge bases and knowledge articles.

For more information about the Knowledge Management roles applicable to Operational Technology Knowledge Management, see Operational Technology Knowledge Management roles.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Create an OT knowledge base

Create an Operational Technology (OT) knowledge base to provide a self-service platform for OT knowledge users to store, share, and manage content that is related to OT incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

Procedure
1. Navigate to **Knowledge** > **Administration** > **Knowledge Bases**.
2. Select **New**.
3. On the knowledge base form, fill in the fields.
   For a description of the field values, see Knowledge base form.
4. Right click the form header and select **Save**.
5. In the related list section, view or configure the items in the following table that are related to the OT knowledge base.

Name	Description
Knowledge	List of knowledge articles that are stored in this knowledge base.
Can Read	List of user criteria that grants read access and enables a user who matches the criteria to read articles in the OT knowledge base.
Can Contribute	List of user criteria that grants contributor access and enables users who match the criteria to create and modify the articles in the OT knowledge base.
Article Templates	If you've activated the Knowledge Management Advanced (com.snc.knowledge_advanced) plugin, the Article Templates related list is displayed. If article templates are in the related list, the articles in that knowledge base can only be created by using one of the article templates listed. If the Article Templates related list is empty, articles can be created by using any article template. Map article templates to the knowledge base by selecting **Edit**. **Note:** Admins, knowledge admins, and knowledge managers can edit the article templates for the knowledge base.
Knowledge categories	List of knowledge categories that are associated with the OT knowledge base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Name	Description
	Note: If the category is marked as inactive, then you can't associate articles to the category. However, it doesn't affect the existing articles of that category.

6. Select **Submit**.

Create the user criteria for an OT knowledge base

Create a user criteria record to determine the users who can read or contribute to an Operational Technology (OT) knowledge base.

Before you begin

Role required: user_criteria_admin

Note: To create a user criteria record from the Knowledge module, you must have the user_criteria_admin role in addition to the knowledge role. For more information about access, see Managing access to knowledge bases and knowledge articles.

About this task

Use the user criteria in Knowledge Management to determine whether certain users can access OT knowledge bases and knowledge articles. After you create a user criteria record, you can assign it to an OT knowledge base to control who can read and contribute to a knowledge base and its articles. You can further assign the user criteria at an article level to control who can read it.

Procedure

1. Navigate to **All** > **Knowledge** > **Administration** > **User Criteria**.
2. Select **New**.
3. On the form, fill in the fields.

User Criteria form

Field	Description
Name	Unique name of the user criteria.
Users	Users who must match the user criteria.
Groups	Groups that must match the user criteria.
Roles	Roles to match the user criteria. **Note:** ○ Because the evaluation of a role is cached in the session, any change in the role requires you to log in again. ○ User criteria are not applicable for elevated privilege roles.
Advanced	Option to display or hide the advanced option that includes the **Script** field on the User Criteria form.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Script	Script to define any additional user criteria that returns true or false. This field is available when the **Advanced** option is selected on the User Criteria form. **Note:** ○ A script is evaluated in the scope that the user criteria are created in. ○ The evaluation of a script is cached in the session, so any change in the evaluation requires you to log in again. If a scripted user criterion is defined for a knowledge base, the user access to the knowledge bases is evaluated after every session. If the script results in changes after a session cache is built, the result takes effect in the next session. ○ Don't use `gs.getUser()` or other session APIs because they cause conflicts when used in diagnostic tools. Use the predefined `user_id` variable available in the script to get the user ID of the user being used to evaluate the script. ○ Scripts are evaluated dynamically. Therefore, including scripts in a user criteria can impact the performance of your system.
Active	Option to activate or deactivate the user criteria.
Companies	Companies that the user record must match.
Locations	Locations that the user record must match.
Departments	Departments that the user record must match.
Match All	Option to determine whether all elements from each populated user criteria field must match. If selected, only the users who match all user criteria are given access. If cleared, the user must meet one or more of the set user criteria to be given access. By default, this check box is cleared so that any condition met provides a match. For example, consider a user criteria record for the following conditions: ○ Locations A or B ○ Company C or D With **Match All** selected, only the users who meet all of these conditions are matched. For example, a user with a location A and a company C. If **Match All** isn't selected, users who meet any of these conditions are matched. For example, a user with a location B. **Note:** If you select **Match All**, ensure that you don't create contradictory conditions that can never be met. For example, if all users in location A work for company G, the conditions in this example can never be met.

4. Select **Submit**.

What to do next

Now you can assign the user criteria to an OT knowledge base. For more information, see Assign the user criteria to an OT knowledge base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Assign the user criteria to an OT knowledge base

Assign the user criteria records to an Operational Technology (OT) knowledge base to control which users can create, read, write, and retire knowledge articles within the knowledge base.

Before you begin

Role required: knowledge_manager, knowledge_admin, or admin

About this task

You can assign user criteria to an OT knowledge base to control read or contribute access.

Procedure

1. Navigate to **All** > **Knowledge** > **Administration** > **Knowledge Bases**.
2. Select the OT knowledge base record that you want to manage.
3. Add the user criteria to the OT knowledge base.
   a. Depending on the user criteria that you want to set, select one or more of the related lists.

Related list	Description
Can Read	Users can read knowledge articles in the knowledge base.
Cannot Read	Users can't read knowledge articles in the knowledge base.
Can Contribute	Users can create, modify, and retire knowledge articles in a knowledge base. Contribute access to a knowledge base also provides read access to all articles in the knowledge base.
Cannot Contribute	Users can't create, modify, retire, or read knowledge articles in the knowledge base.

   b. In the selected related list, add the required user criteria.
      - As a user with the admin role, add a new user criteria record by selecting **New**, specifying the required fields, and selecting **Submit**.
      - As a user with the knowledge_manager, knowledge_admin, or admin role, add an existing user criteria record by selecting **Edit**, moving the required user criteria from the Collection column to the Knowledge column, and selecting **Save**.
4. On the knowledge base form, select **Update**.

Review access to OT knowledge bases for unauthenticated users

Review the Operational Technology (OT) knowledge bases that are accessible to unauthenticated users by using the user criteria and *glide.knowman.block_access_with_no_user_criteria* property settings.

Before you begin

Role required: knowledge_admin or admin

About this task

If you want to restrict unauthenticated users for a knowledge base, you can use the user criteria or the *glide.knowman.block_access_with_no_user_criteria* property settings.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Knowledge** > **Administration** > **Knowledge Bases**.
2. Review the OT knowledge bases that are accessible to unauthenticated users.
3. **Optional:** To restrict unauthenticated users for a knowledge base by using the user criteria, select the knowledge base record and update its user criteria.
   For more information about creating the user criteria, see Create the user criteria for an OT knowledge base. For more information about assigning the user criteria, see Assign the user criteria to an OT knowledge base.
4. **Optional:** Restrict unauthenticated users for a knowledge base by using the *glide.knowman.block_access_with_no_user_criteria* property settings.
   a. Navigate to **All** > **Knowledge** > **Administration** > **Properties**.
   b. Set the *glide.knowman.block_access_with_no_user_criteria* property settings to true.
   c. Select **Save**.

Assigning knowledge workflows to an OT knowledge base

You can assign different Knowledge Management workflows to each Operational Technology (OT) knowledge base for the publishing and retiring processes.

Knowledge workflow overview

You can use the default Knowledge Management workflows in the following table for Operational Technology Knowledge Management and apply them to OT knowledge bases.

Note: For the workflows that require approval, you can configure which users can approve or reject by editing the `getApprovers()` function in the `KBWorkflow` script include.

Default Knowledge Management workflows

Workflow	Description
Knowledge - Approval Publish	Requests approval from a manager of the knowledge base. Articles in approval have a state of **In Review** before moving to a **Published** state after approval. If they're set to publish later, they're moved to a **Scheduled** state. If the manager rejects the request, the workflow is canceled and the article remains in the **Draft** state. If the**ownership groups** option is enabled, email notifications with a link to the article are sent to the ownership group members for approval. If the **ownership groups** option isn't enabled, email notifications with a link to the article are sent to the knowledge base managers for approval. A notification is also sent to the authors or the revisers of the articles to inform them that their article has been approved or rejected.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Default Knowledge Management workflows (continued)

Workflow	Description
	To turn on the approval email notifications, set the *glide.knowman.enable_approval_notification* property to `true`. **Note:** Only the active user receives the notifications.
Knowledge - Approval Retire	Requests approval from a manager of the knowledge base before moving the article to the retired state. If any manager rejects the request, the workflow is canceled and the article remains in the **Published** state. If the **ownership groups** option is enabled, email notifications with a link to the article are sent to the ownership group members for approval. If the **ownership groups** option isn't enabled, email notifications with a link to the article are sent to the knowledge base managers for approval.
Knowledge - Instant Publish	Immediately publishes a draft article without requiring an approval, or publishes on the scheduled publish date if set to publish later.
Knowledge - Instant Retire	Immediately retires a published article without requiring an approval.
Knowledge - Publish Knowledge	Subflow that moves the knowledge article to the **Published** state. You can use this subflow when defining your own workflow.
Knowledge - Retire Knowledge	Subflow that moves the knowledge article to the **Retired** state. You can use this subflow when defining your own workflow.

Email notifications for approval workflows

You can send email notifications for approval workflows.

- Notify approvers about the knowledge articles submitted for their approvals.
- Notify authors about the approval status of their knowledge articles

To send email notifications for approval workflows, enable the **Send notification to approvers and authors in article approval workflow** property (*glide.knowman.enable_approval_notification*). Beginning with the New York release, the property is enabled by default. Existing customers on release versions prior to the New York release can enable this property to send email notifications. Disable any custom notifications for article approvals before enabling this property. If the *glide.knowman.enable_approval_notification* property isn't available, an

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

administrator can create the property and set its value to true. For more information, see Knowledge Management properties.

Reviewing the Knowledge Management property for an Operational Technology knowledge base

As an administrator, you can configure the look and functionalities of Operational Technology (OT) knowledge bases with the Knowledge Management properties.

You can access the Knowledge Management properties by navigating to **All** > **Knowledge** > **Administration** > **Properties**.

Use the property that is listed in the following table to control which roles can flag incomplete or inaccurate articles in knowledge bases.

Glide.knowman.show_flag.roles property

Property	Description
List of roles (comma-separated) that can flag incomplete/inaccurate articles (`glide.knowman.show_flag.roles`)	Enter the role names exactly as they appear in **User Administration** > **Roles**. If both the **Show article rating section** and **Show "Flag Article" option** properties are selected, the users with the roles listed in this property see the flag article option in the article view. All roles listed in this property must also be listed in the **List of roles that can see an article's rating section** property.

For more information about the other available Knowledge Management properties, see Knowledge Management properties.

Using Operational Technology Knowledge Management

After you complete all the required set-up tasks for Operational Technology Knowledge Management, you can begin managing knowledge articles that are related to Operational Technology (OT) incidents.

Operational Technology Knowledge Management overview

By using#Operational Technology Knowledge Management, you can create, edit, and retire knowledge articles depending on the needs of your team. When used with the Operational Technology Incident Management application, you can browse articles that are related to an incident and create articles from an incident.

The following examples show how to apply#Operational Technology Knowledge Management to your team:

- An OT engineer with several years of experience wants to capture their OT device knowledge in one place for guide workers and junior technicians.
- Front-line workers and technicians responsible for production process operations have noticed an issue on the factory floor and need a knowledge article that explains remediation.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Basic Operational Technology Knowledge Management Process

The following workflow describes the basic process for Operational Technology Knowledge Management.

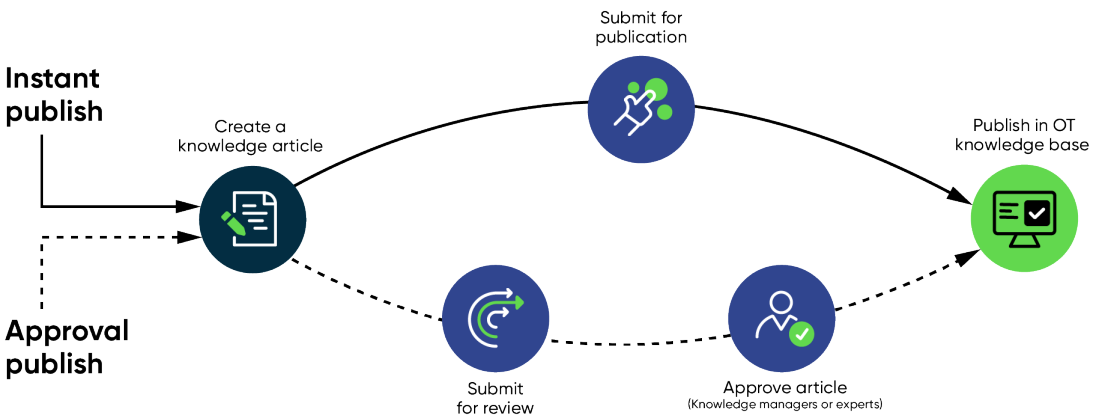
Basic OT Knowledge workflow



Publish a knowledge article

The following workflow describes how a knowledge article is created and published both with (Approve Publish) and without (Instant Publish) approval.

Publish workflow

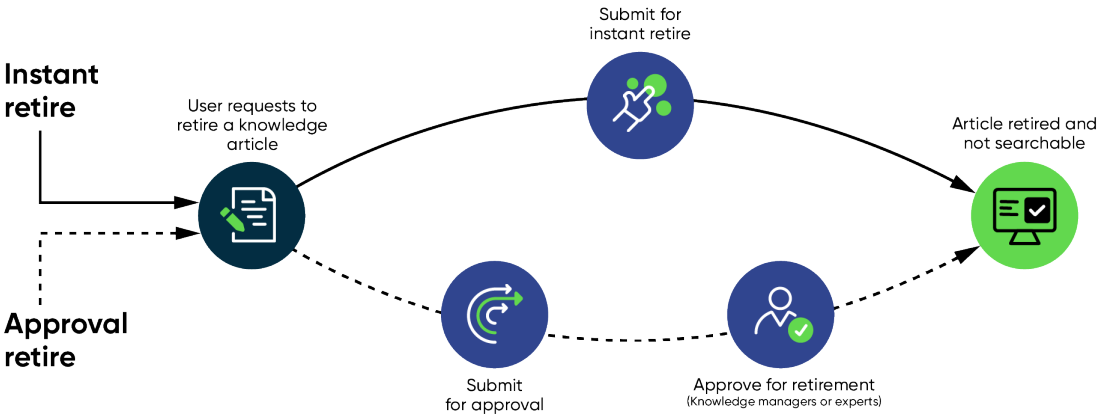


Retire a knowledge article

The following workflow describes how a knowledge article is retired both with (Approve Retire) and without (Instant Retire) approval. The Instant Retire workflow lets you retire articles immediately without needing an approval. The Approval Retire workflow sends an approval request to knowledge managers or experts to make sure that retiring the article is necessary.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

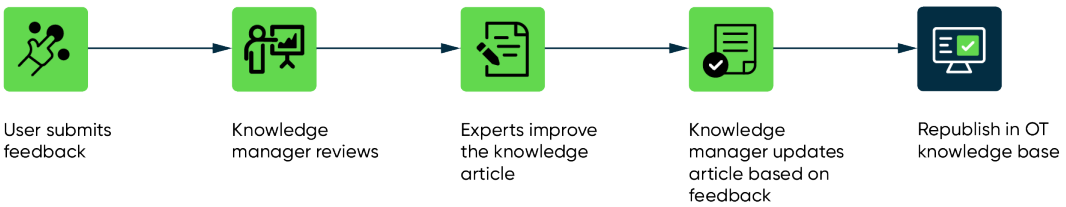
Retire workflow



Review and approve changes to a knowledge article

The following workflow describes how an existing knowledge article is updated with user feedback.

User feedback workflow



Knowledge articles

Knowledge articles provide information about workplace updates, self-help, troubleshooting steps, and other information that your OT team must access. For example, you can create the following knowledge articles for the following cases:

- A standard operating procedure template used throughout your organization.
- Lessons learned during an incident.
- An image that annotates the different production materials.

You can view the knowledge articles in the Industrial Workspace in the following ways:

- Under the Knowledge module in the Industrial Workspace list view.
- In the Agent Assist window when you open an OT incident.
- Using the global search feature in the Industrial Workspace header.

Under the Knowledge module in the Industrial Workspace list view, you can view knowledge articles in the following lists:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: You must be assigned the knowledge role to see these list modules in the Industrial Workspace.

Your unpublished articles

The articles you've created that aren't yet published in the OT knowledge base.

Your published articles

The articles you've created that are published to the OT knowledge base.

All articles

All articles that are available in the OT knowledge base.

Create a knowledge article from an OT incident record

Create a knowledge article to record and save information that is related to an Operational Technology (OT) incident and its resolution.

Before you begin

Role required: sn_ot_incident_write

Note: You also need the **Can contribute** access to at least one knowledge base. For more information, see Create an OT knowledge base.

About this task

Creating a knowledge article directly from an incident record helps to make sure that the knowledge article is linked to the correct incident for contextual information. The knowledge article can also help your team resolve similar incidents in the future when they include the correct procedures, challenges, and solutions.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the list view under the OT Incident module, open one of the available lists.
3. Select the OT incident record that you want to create a knowledge article for.
4. Select the **More actions** icon (⋯) to expand the menu.
5. Select **Create Knowledge**.

   Note: You must set the incident record's state to **Resolved** to see the **Create Knowledge** button.

6. On the form, fill in the fields.

Knowledge article form

Field	Description
Knowledge base	Knowledge base that the knowledge article should be included in. **Note:** If you configured the OT knowledge base's visibility correctly, OT users can find the knowledge base in this reference list.
Category	Classification of the knowledge article.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Short description	Brief description of the incident resolution that is used as the knowledge article title.
Article body	Content of the knowledge article that describes any procedures, challenges, and solutions for the incident.
Valid to	Date that the knowledge article is valid until.

7. Select **Save**.
   The knowledge article is saved as a draft and attached to the parent OT incident.
8. Select **Publish**.

Result

The knowledge article is now published in your OT knowledge base. To view the knowledge article, open the Attached Knowledge related list in the incident record.

Note: If you set the **Publish workflow** field in your OT knowledge base to **Knowledge - Approval Publish**, the article must be approved before being published.

Create a knowledge article in Industrial Workspace

Create a knowledge article in Industrial Workspace to help cater an article's contents to the needs and solutions not directly related to an Operational Technology (OT) incident.

Before you begin

Role required: knowledge

Note: You also need the **Can contribute** access to at least one knowledge base. For more information, see Create an OT knowledge base.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the list view under the Knowledge module, open one of the available lists.
3. Select **New**.
4. On the form, fill in the fields.

Knowledge article form

Field	Description
Knowledge base	Knowledge base that the knowledge article should be included in. **Note:** If you configured the OT knowledge base's visibility correctly, OT users can find the knowledge base in this reference list.
Category	Classification of the knowledge article.
Short description	Brief description of the incident resolution that is used as the knowledge article title.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Field	Description
Article body	Content of the knowledge article that describes any procedures, challenges, and solutions for the incident.
Valid to	Date that the knowledge article is valid until.

5. Select **Save**.
   The knowledge article is saved as a draft and attached to the parent OT incident.
6. Select **Publish**.

Result
The knowledge article is now published in your OT knowledge base.

Note: If you set the **Publish workflow** field in your OT knowledge base to **Knowledge - Approval Publish**, the article must be approved before being published.

Report a knowledge gap from an OT incident record

Report a knowledge gap from an Operational Technology (OT) incident if you can't find relevant knowledge articles about the incident.

Before you begin
Role required: sn_ot_incident_read

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the list view under the OT Incident module, open one of the available lists.
3. Select the incident record that you want to report a knowledge gap for.
4. Select the **More actions** icon (...) to expand the menu.
5. Select **Report Knowledge Gap**.
6. On the form, fill in the **Description** field with a summary of the knowledge gap.

   Note: The **Topic** field automatically fills with the name of the incident record. If needed, you can change this field.

7. Select **Submit**.

Result
The knowledge gap is reported and a feedback task is created.

What to do next
You can view the feedback task under the Knowledge Gaps related list in the incident record.

To assign feedback tasks to the correct user or user group, see Assign feedback tasks.

Approve requests to publish or retire a knowledge article

Approve requests to publish or retire a knowledge article to help ensure that the knowledge base is up to date.

Before you begin
Role required: knowledge_manager

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task
If you're assigned as the manager of an OT knowledge base receive, you can receive approval requests for the publishing and retiring of articles that belongs to the knowledge base.

Procedure
1. Open the email notification regarding the approval request.
2. Select the link in the email to open the request.
3. Approve or reject the request.
4. **Optional:** If rejected, leave a comment explaining why the article request was rejected.

Result
The user who created the approval request is notified via email.

Assign feedback tasks

Assign feedback tasks to a user to help make sure that the feedback task is addressed and the related knowledge article is updated.

Before you begin
Role required: knowledge_manager

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. In the list view under the Knowledge module, open the Unassigned OT Knowledge Gaps list.
3. Select the feedback task that you want to assign to a user or assignment group.
4. In the **Assigned to** field, add the user that you want to assign the feedback task to.
5. Select **Save**.

Result
The assigned user can now view the feedback task in the My Feedback Tasks list under the Knowledge module list view.

To view other assigned feedback tasks, select the Assigned Feedback Tasks list under the Knowledge module list view in the Industrial Workspace.

To view the unassigned OT knowledge gaps, select the Unassigned OT Knowledge Gaps list under the Knowledge module list view in the Industrial Workspace.

Find information in the related knowledge articles for an OT incident

Find information in the related knowledge articles that are attached to an Operational Technology (OT) incident record for any previous resolutions that may be applicable.

Before you begin
Role required: sn_ot_incident_read

Note: You must have the sn_ot_incident_read role and read access to the knowledge base that contains the articles that match the context of this incident.

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. In the list view under the OT Incident module, open an available list.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select the incident record that you want to view.
4. In the incident record, select the Agent assist button to open the Agent Assist window if it's not already opened.
5. To view the full knowledge article, select the **More actions** button ⋯.
6. Select **Full View**.
7. **Optional:** To attach the knowledge article to the open incident record, select **Attach** in the Agent Assist window.
8. **Optional:** To flag the knowledge article, select **Flag** in the Agent Assist window.
9. **Optional:** To mark the knowledge article as helpful, select the **More actions** button ⋮ and choose **Helpful**.

Operational Technology Knowledge Management reference

Reference topics provide additional information about Operational Technology Knowledge Management.

Operational Technology Knowledge Management roles

You can assign Knowledge Management roles to your Operational Technology Knowledge Management users.

The following table lists the Knowledge Management roles that you can assign to your users so that they can access Operational Technology Knowledge Management capabilities.

Knowledge Management roles applicable to Operational Technology Knowledge Management

Role	Description
knowledge	The knowledge role can contribute to the default knowledge base and access the Knowledge application menu. The knowledge role is a fulfiller role and not a requester role. **Note:** Requesters can view, comment, and give feedback to the knowledge articles. However, a requester can't create or edit articles.
knowledge_manager	The knowledge manager can perform administrative functions for the knowledge bases that they manage, such as defining the categories, pinning the important articles, and approving the changes to the articles. Users selected as managers of a knowledge base receive this role automatically. **Note:** The knowledge role comes as a subordinate role.
knowledge_admin	The knowledge administrator can perform all the administrative tasks that are associated

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Knowledge Management roles applicable to Operational Technology Knowledge Management (continued)

Role	Description
	with maintaining the Knowledge Management system. **Note:** • A user selected as a knowledge admin can make changes to all the knowledge bases except the scoped knowledge base. • The knowledge role comes as a subordinate role.

Knowledge base form

When creating a new knowledge base, fill out the following form fields.

Knowledge base form fields

Field	Description
Title	Unique name for the Operational Technology (OT) knowledge base.
Article Validity	Number of default days that the articles are valid for after the date that they're created.
Icon	Image that provides a visual reference to describe the OT knowledge base. The image is displayed next to all articles from this knowledge base in the article search results page.
Disable commenting	Option to disable commenting. If selected, users can't comment on articles in the OT knowledge base.
Disable suggesting	Option to disable edit suggestions. If selected, users can't suggest edits to articles in the OT knowledge base.
Disable category editing	Option to disable the editing of OT knowledge categories. If selected, only OT knowledge managers can add or edit the knowledge categories for the OT knowledge base.
Disable rating	Option to disable the rating for articles. If selected, users can't rate the article in the OT knowledge base.
Disable mark as helpful	Option to disable the mark as helpful. If selected, the user can't mark any article as helpful in the OT knowledge base.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Knowledge base form fields (continued)

Field	Description
Enable blocks	Option to enable the knowledge blocks feature. If selected, you can create knowledge blocks to add to knowledge articles within the OT knowledge base.
Checklist	Checklist to evaluate the quality of articles in the OT knowledge base.
Application	Application scope of the OT knowledge base.
Owner	User responsible for the OT knowledge base. A knowledge base owner can assign other roles to the knowledge base.
Managers	Users who perform administrative functions on the OT knowledge base.
Publish workflow	Workflow for publishing the articles in the knowledge base: • **Knowledge - Instant Publish**: Publishes articles in the knowledge base without requiring an approval. • **Knowledge - Approval Publish**: Requests an approval from the manager of the knowledge base before moving the articles to the published state.
Retire workflow	Workflow for retiring the articles in the OT knowledge base: • **Knowledge - Instant Retire**: Retires the articles in the knowledge base without requiring an approval. • **Knowledge - Approval Retire**: Requests an approval from the manager of the knowledge base before moving the articles to the retired state.
Active	Option to indicate that the OT knowledge base is active. If not selected, only users with the admin role or knowledge administrators can create, search for, or view its articles.
Description	
Set default knowledge field values	Default configuration settings for the OT knowledge base.
Related products	List of products that are related to the OT knowledge base content.

Related information

Find more information about the OT extension classes and related applications.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Operational Technology (OT) extension classes

The CMDB updates classes for OT.

Related applications

Knowledge Management

The Knowledge Management application enables the sharing of information in knowledge bases. These knowledge bases contain articles that provide users with information such as self-help, troubleshooting, and task resolution.

Operational Technology Incident Management

The Operational Technology Incident Management application enables manufacturers to manage OT device incidents from the time the incident is opened to when it's complete.

IT Service Management

When integrated with Operational Technology Knowledge Management, the ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Operational Technology Request Management

Operational Technology Request Management lets you request catalog items and fulfill them based on the defined flows.

Explore  Exploring Operational Technology Request Management	Configure  Plan and configure your implementation
Use  Using Operational Technology Request Management	Reference  Get details about related information and applications

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring Operational Technology Request Management

Operational Technology Request Management lets you access the Operational Technology (OT) Service Catalog to request OT catalog items and fulfill them based on the defined flows. OT workers can then create and submit an OT request from a catalog item, which helps provide a consistent experience and facilitates cross-functional requests.

Operational Technology Request Management overview

Watch an overview about the Operational Technology Service Management product suite to learn more about the Operational Technology Request Management.
https://player.vimeo.com/video/1019801515?badge=0&autopause=0&player_id=0&app_id=58479

Operational Technology Request Management benefits

With Operational Technology Request Management, you can apply the following benefits to your OT system and help your team manage catalog requests:

- Provides a single view to efficiently manage multiple catalog requests.
- Encourages transparency, expedites request processes, and minimizes delays with automatic notifications and approvals.
- Maintains the products and services menu that you can use to create and update catalog requests.

Applying Operational Technology Request Management to your OT system

You can apply Operational Technology Request Management to your Operational Technology (OT) system to enable other users to create and submit OT requests for OT products and services.

Operational Technology Request Management overview

Operational Technology Request Management lets you request catalog items and fulfill them based on the defined flows. OT workers can then create a request in the OT Service Catalog and choose the catalog item that best fits their needs.

Use cases

The following table describes different OT personas and how they can use Operational Technology Request Management.

Operational Technology Request Management use cases

Persona	Description
OT engineer	Can use Operational Technology Request Management to file and manage OT requests for various OT products and services in a one place. A few examples of the catalog items that can be requested are third party remote access, new OT PCs, new OT devices, and new OT host connections.
Plant head or supervisor	Can use Operational Technology Request Management to engage with the correct team

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Request Management use cases (continued)

Persona	Description
	to remediate an incident reported on the factory floor.

Configuring Operational Technology Request Management

Configure Operational Technology Request Management so that you can create the data foundation for the Operational Technology (OT) solution.

If you have the admin role, you can use Guided Setup to lead you through the setup of Operational Technology Request Management. Guided Setup is a tool that assists with application or capability configuration. It organizes the configuration activities into categories. These categories contain the information about the setup tasks, steps to complete each task, and links to the pages in your instance where you perform the configuration. The links to useful help content are also provided.

To access Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

The following table lists the Guided Setup tasks and their purposes for Operational Technology Request Management.

Note: Operational Technology Request Management is included with the Industrial Workspace Common. No additional plugins are needed.

The following table shows the tasks that your users must complete for a successful setup and configuration.

Operational Technology Request Management setup tasks

Task	Purpose
Load demo data.	To load the demo data for Operational Technology Request Management, you must load the demo data of the Industrial Workspace Common plugin. To load the demo data, complete the following steps. 1. Navigate to **All** > **System Definition** > **Plugins**. 2. In the search bar, search for the `Industrial Workspace Common` plugin. 3. Once the results load, select the **Installed** tab and open the Industrial Workspace Common page. 4. Under **Quick Actions**, select **Load demo data**.
Assign Operational Technology Request Management roles.	Assigns the roles to control the actions that are available for each user.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Request Management setup tasks (continued)

Task	Purpose
Create catalog items for your OT service catalog using the catalog builder.	Create catalog items for the OT Service Catalog using the catalog builder. Other users can also submit their OT requests and choose the catalog item that best fits their needs.
Add catalog item categories for the catalog items you create in the OT Service Catalog.	Select different categories for the catalog items you create in the OT Service Catalog to organize OT catalog items into logical groups.
Create a fulfillment flow for an OT request in Workflow Studio.	Create a fulfillment flow with catalog tasks in Workflow Studio for your catalog item as needed to fulfill an OT request.

Assign roles to your Operational Technology Request Management users

Assign roles to your users so that you can control their access to the features, capabilities, and data for Operational Technology Request Management.

Before you begin

Role required: admin

About this task

For more information about the Operational Technology Request Management roles you can assign to your users, see Components installed with Operational Technology Request Management.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Catalog item categories

You can select different categories for the catalog items you create in the Operational Technology (OT) Service Catalog. Categories help organize OT catalog items into logical groups. When requesters submit an OT request, they can choose the catalog item that best fits their needs based on its designated category.

If needed, you can define categories and subcategories to organize the OT catalog items and help users locate the products and services they need. For more information about how to define catalog item categories, see Create a category.

Create a catalog item for your Operational Technology Service Catalog

Create a catalog item for the Operational Technology (OT) Service Catalog using the catalog builder so that other users can submit OT requests categorized by catalog item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: admin

About this task
You can create catalog items for the OT Service Catalog in the catalog builder. When other users submit an OT request, they can choose the catalog item that best fits their needs. For example, requesting remote access to an OT device can be a catalog item available in the OT Service Catalog. This allows third parties to work on issues related to OT devices.

Procedure
1. Navigate to **All** > **Service Catalog** > **Catalog Builder**.
2. In the **Dashboard** tab under **Start creating your new catalog item**, select **Create a new catalog item**.
   Alternatively, select the **Catalog Items** tab and click **New**.
3. On the **Getting Started** page, select **Continue**.
4. On the **Select your item template** page, select the **OT Catalog Item Template**.
5. Select **Use this item template**.
6. On the **Create catalog item** form, fill in the fields.

   For more information about the Catalog Item form fields, see Operational Technology Catalog Item form.

   Note: You can't remove the OT Catalog Item Variable Set from the Questions section. The OT Catalog Item Variable Set is what distinguishes OT requests from other requests. You can instead create new questions for your item form by selecting **Insert New Question**. For more information about inserting a new question, see Create a question for a catalog item in Catalog Builder.

7. **Optional:** To preview your catalog item, select **Preview**.
8. **Optional:** To save your progress, select **Save**.
9. Once you get to the **Review and Submit** section, review the catalog item information you added and select **Submit**.
10. Repeat steps 1 to 9 for each catalog item that you want to create.

Result
The catalog item is created and available for other users to select when they create an OT request in the OT Service Catalog.

Create a fulfillment flow for an Operational Technology request

Create a fulfillment flow with catalog tasks in Workflow Studio for your catalog item as needed to fulfill an Operational Technology (OT) request.

Before you begin
Role required: admin

About this task
You can link a fulfillment flow to your catalog item. Fulfillment flows trigger catalog task creation and notifications when another user submits an OT request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Process Automation** > **Flow Designer**.
2. Select the **Flows** button.
3. In the **New** drop-down, select **Flow**.
4. On the **Properties** form, fill out the fields.
   For more information about the **Properties** form, see Create a flow in Workflow Studio.
5. Select **Build Flow**.
6. Add a trigger to your flow.
   For more information, see Create a flow in Workflow Studio.
7. Add actions, flows, subflows, or glow logic.
   For more information, see Create a flow in Workflow Studio.
8. Select **Save**.

Result

Workflow Studio saves a draft of the flow, trigger, and actions for the fulfillment flow. You can now choose the fulfillment flow and apply it to a catalog item.

Using Operational Technology Request Management

After you complete all the required set-up tasks for Operational Technology Request Management, users can begin creating and managing Operational Technology (OT) requests.

Create an Operational Technology request on the Industrial Workspace

Create an Operational Technology (OT) request in the Industrial Workspace to address a product or service needed for an OT device or incident.

Before you begin

Role required: any OT user

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the **OT Requests** list module, select the **My Requests** list.

> **Note:**
>
> The **My Requests** list is accessible to all the OT users that can access the Industrial Workspace.

4. Select **New**.
5. In the OT Service Catalog, select one of the available catalog items that best fits your needs.
6. Fill in the fields as needed for your request.
7. Select **Request**.

What to do next

Once the OT request is submitted, you receive an email with the details of your request. You can use the link provided in the email to open the request record and track its status. You can also edit the request record with further context needed to complete the request.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If there are any changes made to the request record, you're notified with an email describing the changes made. For example, work notes were added to the record, or its state was updated.

Operational Technology Request Management lists in the Industrial Workspace

You can view your Operational Technology (OT) requests and catalog tasks in the Industrial Workspace list view.

OT requests

The following lists are available to view and access OT requests in the Industrial Workspace list view under the **OT Request** module.

Note: You must have the sn_request_read role to access these lists.

OT Request lists

List	Description
My Requests	OT requests raised by you or for you by the Administrator.
Open Request Items	All OT requests

OT catalog tasks

You can view your OT catalog tasks in the lists available under the **OT Tasks** module. For OT catalog tasks, the **Task type** column value is **Catalog Task**.

Operational Technology Request Management reference

Reference topics provide additional information about Operational Technology Request Management.

Components installed with Operational Technology Request Management

Several types of components may be installed with the activation of Operational Technology Request Management, including user roles and service catalogs.

Roles installed

Operational Technology Request Management roles

Name	Description	Contains roles
sn_request_read	Read access to the Request (sc_request,) Requested Item (sc_req_item) or Catalog Task (sc_task).	NA
sn_request_write	Write access to the Request (sc_request,) Requested Item (sc_req_item), or Catalog Task (sc_task).	• task_editor • dependency_views • agent_workspace_user • view_changer

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Request Management roles (continued)

Name	Description	Contains roles
		• cmdb_read • cmdb_query_builder_read • sn_request_read
sn_request_comment_write	Write access to the comments for the Requested Item (sc_req_item). **Note:** The sn_request_comment_write role alone does not give access to comments write, you will need write access for the table.	NA

Service catalogs installed

Operational Technology Request Management service catalog

Name	Description
OT Service Catalog	Service catalog provided for users to submit OT requests.

Operational Technology Catalog Item form

When creating a new catalog item for the Operational Technology (OT) Service Catalog, fill out the following form fields.

The following tables describe the fields available in each section of the OT Catalog Item form.

Details

Field	Description
Basic Info	
Item name	Name to appear in the catalog.
Short description	Text that appears on the service catalog homepage, search results, and the title bar of the order form.
Item details	
Image	Image of the item.
Description	Full description of the item. This description appears in the catalog when a user selects the item or clicks the associated **Preview** link.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Details (continued)

Field	Description
	You can embed videos, images, links to internal knowledge base (KB) articles, and links to external sources of information and instruction documentation.

Location

Field	Description
Catalogs	
Selected catalogs	Catalogs this item appears in.
Categories	
Selected categories	Category for the item. Categories can only be selected after the **Catalogs** field is populated. Catalog searches find only items assigned to a category in the Service Portal.
Topics	
Selected topics	Topics for the item. Requesters can use the topics you added to find and access the catalog item once the catalog item is published.

Questions

Field	Description
OT Catalog Item Variable Set	
Site	Site that's affected by the catalog item.

Settings

Field	Description
Portal settings	
Submit button label	Label for the submit button after the requester finishes filling out the catalog item form.
Hide 'Add to cart' button	If selected, the **Add to Cart** button is not displayed for the item. If the **Show Add to Cart** instance option of the widget is set to false, then this setting is ignored. This setting is selected by default if the **Request method** is **Request** or **Submit**. For upgrade scenarios, if the **No cart** field is selected in Platform, run the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Settings (continued)

Field	Description
	`CatalogPortalSettingsMigration` script include to update this setting to the **Hide 'Add to Cart'** field in the **Portal Settings** tab. **Note:** Applicable for a catalog item and order guide.
Hide ‘Save as draft’ button	If selected, the **Save as draft** button is not displayed for the item.
Hide quantity selector	If selected, the **Quantity** list is not displayed for the catalog item. This is selected by default if the **Request method** is **Request** or **Submit**. For upgrade customers, if the **No quantity** field is selected in Platform, run the `CatalogPortalSettingsMigration` migration script to update this setting to the**Hide Quantity** field in the **Portal Settings** tab. **Note:** Applicable for a catalog item. An order guide inherits this setting from the included catalog item.
Hide delivery time	If selected, the **Delivery Time** field is not displayed for the catalog item. This is selected by default if the **Request method** is **Submit**. **Note:** Applicable for a catalog item. An order guide inherits this setting from the included catalog item.
Hide attachment button	If selected, the **Add attachments** button is not displayed for the catalog item. **Note:** Applicable for a catalog item and record producer. An order guide inherits this setting from the included catalog item.
Make attachment mandatory	If selected, adding an attachment is mandatory for the catalog item.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Settings (continued)

Field	Description
	Note: Applicable for a catalog item and record producer.

Access

Field	Description
Available for	
User criteria granted access	Select the user criteria that can access the catalog item.
Not available for	
User criteria denied access	Select the user criteria that cannot access the catalog item.

Fulfillment

Field	Description
Fulfillment method	
Process engine	Sequence for item request fulfillment.
Selected flow	Flow that defines how the item request is fulfilled. **Note:** This field is only visible if you select **Flow Designer Flow** in the **Process engine** field.
Selected workflow	Workflow that defines how the item request is fulfilled. **Note:** This field is only visible if you select **Workflow** in the **Process engine** field.

Related information

Find more information about the Operational Technology (OT) extension classes and related applications.

Extension classes overview

The extension classes help you understand how Operational Technology Management works with the Configuration Management Database (CMDB).

Operational Technology (OT) extension classes

The CMDB updates classes for OT.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related applications

Request Management

Request Management allows catalog items to be requested and fulfilled based on defined flows.

IT Service Management

The ServiceNow IT Service Management application enables engineers to resolve OT device and production process issues quickly.

Recommended Actions for Operational Technology Service Management (OTSM)

Recommended Actions for Operational Technology Service Management (OTSM) allows you to set up and apply real-time actionable recommendations. This speeds up the triaging process and resolves issues quickly across various records in the Industrial Workspace, including Operational Technology (OT) incidents.

Get started

Explore	Configure	Use
		
Learn how Recommended Actions for OTSM can help you manage your OT system.	Set up and configure Recommended Actions for OTSM to meet your specific needs.	Manage your OTSM records with Recommended Actions for OTSM.

Helpful resources

Some ServiceNow resources that can provide you with helpful information are:

ServiceNow Store

https://store.servicenow.com/sn_appstore_store.do#!/store/home

Support

Exploring Recommended Actions for Operational Technology Service Management (OTSM)

Recommended Actions for Operational Technology Service Management (OTSM) allows you to set up and apply real-time actionable recommendations for speeding up the triaging process and resolving issues quickly across various records, including Operational Technology (OT) incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Recommended Actions for OTSM overview

Recommendations appear as actionable real-time recommendation in the side panel while updating or creating OT incident records in the Industrial Workspace. You can access recommendations in the Industrial Workspace by selecting the **Recommendations** icon ( ) in the side panel.

Recommended Actions for OTSM workflow

The workflow for Recommended Actions for OTSM includes the Use Context. Use the OT incident context to find and use the recommendations in Industrial Workspace.

Note: For OT incidents, you can use guidance based recommendations in the **Recommendations** panel.

Recommended Actions for Operational Technology Service Management (OTSM) overview

Recommended Actions for Operational Technology Service Management (OTSM) includes the following context components used to configure Recommended Actions for various records in the Industrial Workspace, including Operational Technology (OT) incidents.

Contexts in Recommended Actions for OTSM

#A context enables you to see recommendations for a specific type of record when certain rules are met. These recommendations can help you by suggesting actions to take based on the record context.#For more information, see Contexts in Recommended Actions.

The OTSM context ships the OT incident context described in the following table.

Contexts description

Context	Description
OT incident context	This shows all valid recommendations on OT incidents based on the active recommendations in the Industrial Workspace.

Note: To create a context, see Create a context in Recommended Actions.

Search result mappings

The search result mappings appear in AI search results for OT incident records in the Industrial Workspace.

The OTSM context includes the following search result mappings based on context type:

OT incident: Knowledge [kb_knowledge], OT Incident [sn_ot_incident]

Search Application Configuration

The OTSM context includes the **[AIS] Recommended Actions for OTSM Search Config**. This application supports the AI search for various records in the Industrial Workspace, including OT incidents.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Configuring Recommended Actions for Operational Technology Service Management (OTSM)

Enable a user working on the relevant recommendations provided by Recommended Actions for Operational Technology Service Management (OTSM)

Recommended Actions for OTSM is provided as a new feature for the Operational Technology Incident Management application.

Set up Recommended Actions for Operational Technology Service Management (OTSM)

Set up recommended actions to display relevant recommendations in the Industrial Workspace.

Before you begin

Role required: admin

Procedure

1. Create a rule in Recommended Actions for OTSM.
   OTSM enables you to create new rules. For more information, see Create a rule in Recommended Actions.
2. Create a recommendation.

   OTSM enables you to create new recommendations. For more information, see Create a recommendation in Recommended Actions.
3. Create a resource generator.

   OTSM enables you to create new resource generators. For more information, see Create a resource generator in Recommended Actions.
4. Create Guidance and field recommendations.
   OTSM enables you to configure or create guidance and field recommendations. For more information, see Creating guidance and field recommendation in Recommended Actions.

Configure AI Search for Operational Technology Service Management

Configure AI Search for Recommended Actions for Operational Technology Service Management (OTSM) to enable intelligent query features that help you quickly find the answers you need for OT incidents.

Before you begin

Role required: admin

About this task

For Operational Technology Service Management users, you must define the OT incident [sn_ot_incident] table as an indexed source in order to use AI Search for OT incident records. For more information about indexing, see Indexed sources in AI Search.

Note: Knowledge [kb_knowledge] is also used as an indexed source for Recommended Actions for OTSM, but Knowledge is already indexed.

To define indexed sources, you can use the Guided Setup for AI Search. The following procedure describes how to access the **Define indexed sources** task. For more information about the Guided Setup for AI Search, see Configuring AI Search.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **AI Search** > **Guided Setup**.
2. In the **Define Searchable Content** section, select the **Define indexed sources** task.
3. Select **Configure**.
4. In the **AI Search Indexed Sources** list, select the OT Incident record.
5. Select the **Index Selected Table/s** button.

Using Recommended Actions for Operational Technology Service Management (OTSM)

After you complete all the required set-up tasks for Recommended Actions for OTSM, users can begin utilizing recommended actions for Operational Technology (OT) incidents.

Apply Recommended Actions to your Operational Technology incidents

Apply Recommended Actions to your Operational Technology (OT) incidents to display relevant actions to users based on the context of an OT incident record.

Before you begin

Role required: sn_ot_incident_write

Note: You can only view the recommended actions for an OT incident when the OT incident is related to a site that you have access to, or the incident isn't in a **Closed** or **Canceled** state.

About this task

You can use the Recommendations panel and AI search when viewing an OT incident record to view and select relevant actions related to your incident.

For more information about Recommended Actions, see Using the Recommended Actions application.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the OT Incidents list module, select one of the available lists.
4. Open the incident record that you want to review the recommended actions for.
5. Select the **Recommended Actions** ( ) icon.
6. In the **Recommendations** panel, review and select the recommended actions.

AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

The AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM) feature accesses external sources related to an Operational Technology (OT) incident, and contextualizes how the document is relevant to the incident.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Get started

Explore	Configure	Use
		
Learn how you can use the AI Enhanced Recommended Actions for OTSM feature	Set up the AI Enhanced Recommended Actions for OTSM feature so it's available in the Industrial Workspace	Use AI Enhanced Recommended Actions for OTSM in the Industrial Workspace

AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

The AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM) feature accesses external sources related to an Operational Technology (OT) incident, and contextualizes how the document is relevant to the incident.

AI Enhanced Recommended Actions for OTSM overview

AI Enhanced Recommended Actions for OTSM leverages the external content connector to collect data from an external source. This feature currently supports using Microsoft SharePoint Online as the external source.

Note: The external content connector is part of the existing ServiceNow AI Platform capabilities. For more information about the external content connector, see External Content Connectors.

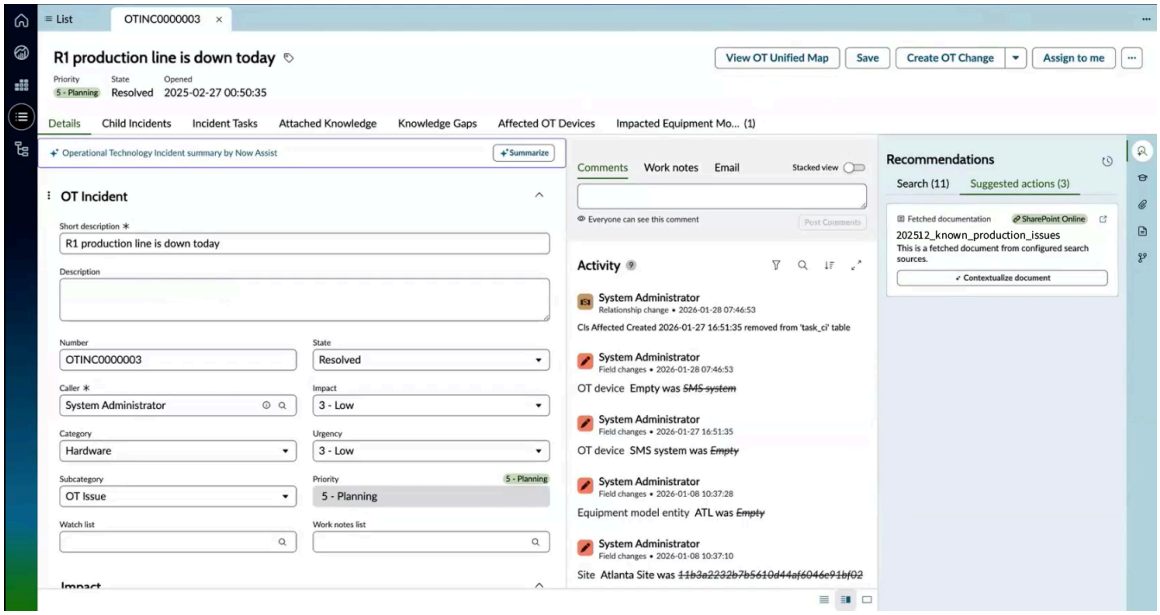
Using the AI Enhanced Recommended Actions for OTSM for your recommended actions

Contextualize document feature

AI Search fetches the data from the external source. Then AI Enhanced Recommended Actions for OTSM displays the fetched data as search results in the **Suggested Actions** tab of the Recommendations panel. You can use the **Contextualize document** UI action in the **Suggested Actions** tab to summarize why a fetched document is relevant to your search prompt.

By default, AI Search uses the short description, description, site, OT device, and equipment model entity field values to display the most relevant external sources for your OT incident. The following image shows an example of what the **Contextualize document** UI action looks like in an existing OT incident record in the Industrial Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



What to explore next

To learn more about configuring and using AI Enhanced Recommended Actions for OTSM, see:

- Configure AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)
- Contextualize an external document

Configure AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

Configure AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM) to contextualize external sources related to an Operational Technology (OT) incident.

Configuration overview

1. Create a Microsoft SharePoint Online external content connector

   Create a Microsoft SharePoint Online external content connector to use as the external source.

2. Configure crawl settings for a Microsoft SharePoint Online external content connector

   Configure the crawl settings to specify the sites you want your Microsoft SharePoint Online external content connector to crawl.

3. Set up the search source

   Set the search source in the **[RA-OTSM AI] Search Profile** record to the Microsoft SharePoint Online external content connector you created.

4. Edit the fields used for search results

   If needed, add or remove the OT incident record fields leveraged during the search process.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Set up AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

Set up AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM) so that you can contextualize external sources related to an Operational Technology (OT) incident.

Before you begin

Ensure you have Recommended Actions for OTSM installed and configured. For more information, see Set up Recommended Actions for OTSM.

Role required: admin

Procedure

1. Create a Microsoft SharePoint Online external content connector.
2. Configure crawl settings for a Microsoft SharePoint Online external content connector.
3. Set up the search source.
   a. Navigate to **All** > **AI Search** > **Search Experience** > **Search Profiles**.
   b. Find and select the **[RA-OTSM AI] Search Profile** record
   c. In the search profile record, select the **Search Sources** tab.
   d. Select **Create and link**.
   e. In the **Indexed source** field, select **SharePoint Online**.

      For more information about the additional form fields, see Search Source form.
   f. Select **Submit**.
4. If needed, add or remove the OT incident record fields that are later used to produce search results.

   Note: If you edit the fields later, the search process restarts so you can view the updated search results.

   a. Navigate to **All** > **Recommended Actions** > **Context**.
   b. Select the **OT incident context** record.
   c. In the context record, select the **Rules** tab.
   d. Select the **OT incident being active** rule.
   e. In the rule record next to **Fields affecting this rule**, select the **Unlock fields affecting this rule** icon.
   f. Using the Add item and Remove item icons, add or remove fields as needed.
   g. Select **Save**.

What to do next

After you set up AI Enhanced Recommended Actions for OTSM, you can use the feature in the Industrial Workspace. For more information see, Contextualize an external document.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM)

After you configure AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM), you can use the feature to contextualize external sources related to an Operational Technology (OT) incident.

Contextualize an external document

With the AI Enhanced Recommended Actions for Operational Technology Service Management (OTSM), contextualize an external document to get an explanation of why the document is relevant to an Operational Technology (OT) incident.

Before you begin

Role required: sn_ot_incident_write

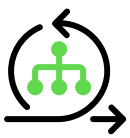
Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the Industrial Workspace list view.
3. In the OT Incidents list module, select one of the available lists.
4. Open the incident record that you want to view the recommended actions for.
5. In the Recommendations panel, select the **Suggested actions** tab to view the suggested action search results for your OT incident.
6. To view why the document was selected, select the **Contextualize document** UI action.
   A summary appears that explains why the selected document is relevant to your OT incident.

Employee Center for OT

The Employee Center for Operational Technology (OT) is a central location where you can submit requests related to OT and industrial services.

Get started

Explore	Configure	Use
		
Learn about the features of the Employee Center for OT	Plan and configure your implementation of the Employee Center for OT	Utilize the Employee Center for OT to help manage your OT system

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploring the Employee Center for OT

The Employee Center for Operational Technology (OT) is a central location in the Employee Center where you can submit requests for industrial issues.

Employee Center for OT overview

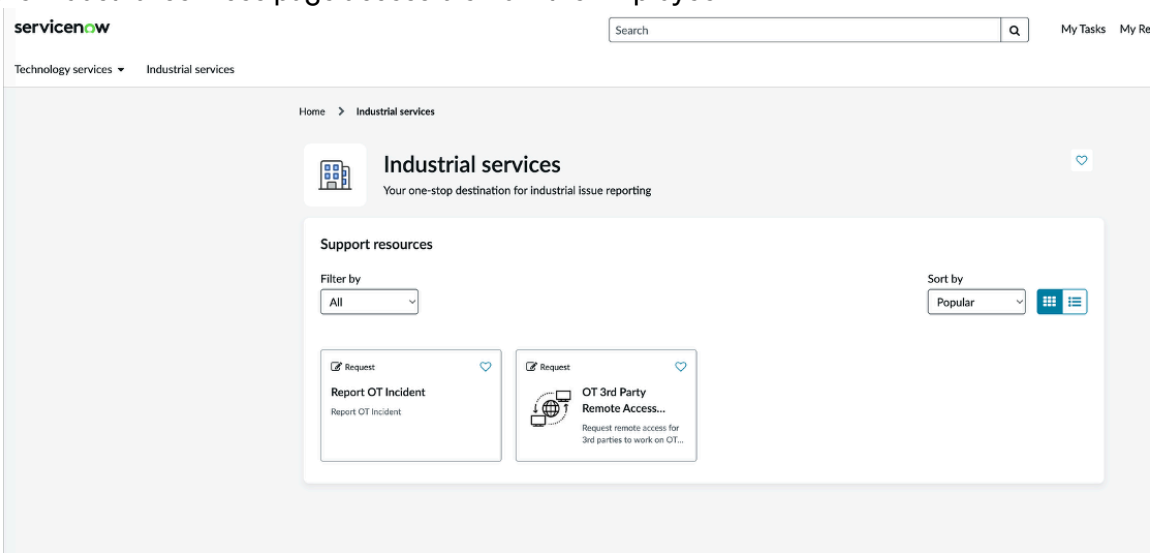
The Employee Center for OT provides you with self-service options to deflect issues, and helps drive productivity and satisfaction by providing simple and immediate access to different resources that can help you manage your OT system. You can use the Employee Center for OT for the following:

- Report an OT incident with an OT incident role
- Search for knowledge articles

The Employee Center for OT is available in the existing Employee Center.

Note: For more information about the Employee Center, see Employee Center.

You can access it by navigating to **All** > **Self-Service** > **Employee Center** and selecting the **Industrial services** tab. The following image shows the Industrial services page accessible from the Employee Center.



You can access the Employee Center for OT on both the desktop and the Now Mobile app experience. Providing both the desktop and mobile app experience helps different OT personas access the Employee Center for OT no matter their location.

Note: For more information about the Now Mobile app experience, see Now Mobile app.

Employee Center for OT features

Feature	Description
Report an OT incident without an OT incident role	Use the Report OT incident option to report an OT incident in real time, if you're not assigned an OT incident role.
Search knowledge articles	If you're looking for additional information, you can search

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Feature	Description
	for knowledge articles directly in the Employee Center using keywords.

What to explore next

To learn more about configuring and using the Employee Center for OT, see:

- Configuring the Employee Center for OT
- Report an OT incident in the Employee Center for OT

Configuring the Employee Center for OT

Configure the Employee Center for Operational Technology (OT) so that you and other users can access the options available in the portal.

Configuration overview

1. To access the Industrial services page, assign the **cmdb_ot_viewer** role.

   Users must be assigned the **cmdb_ot_viewer** role to access the **Industrial services** tab of the Employee Center and successfully submit a request.

   For more information about how to assign roles, see Assign a role to a user.

2. Install and configure the Operational Technology Incident Management.

   Install and configure the Operational Technology Incident Management application needed to use the **Report an incident** request.

   For more information about installing and configuring the application, see Configuring Operational Technology Incident Management.

3. Add more connected content to the Employee Center for OT.

   You can optionally add content to the Industrial services topic page as needed for your organization. For more information about how to add content in the Employee Center, see Add menu items to primary navigation.

Using the Employee Center for OT

After you set up the Employee Center for Operational Technology (OT), you can use the portal to submit requests for industrial issues.

Report an OT incident in the Employee Center for OT

If you're not an Operational Technology (OT) incident user and need to report an OT incident, report the incident in the Employee Center for OT.

Before you begin

Role required: cmdb_ot_viewer

About this task

As a user without an OT incident role, you can still report an OT incident as long as you're assigned the **cmdb_ot_viewer** role. By reporting the OT incident in the Employee Center for OT, an OT incident record is created in the Industrial Workspace. This request is available on both desktop and the Now Mobile app experience.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. To report an OT incident on desktop, complete the following steps.
   a. Navigate to **All** > **Self-Service** > **Employee Center**.
   b. Select the **Industrial services** tab.
   c. On the Industrial services page, select the **Report OT incident**.
   d. On the form, fill out the fields.

Report OT incident form fields

Field	Description
Short description	Brief description of the incident.
Site	Site where the OT incident occurred.
Equipment model entity	Affected equipment model entity. This field is optional.
OT device	Affected OT device.
Description	Detailed explanation of the incident. This field is optional.
Add attachments	Attachments needed for the OT incident, if any.

   e. To save the incident as a draft and come back to it later, select **Save as draft**.
   f. When you're ready to submit the incident, select **Submit**.
2. To report an OT incident on the Now Mobile app, complete the following steps.
   a. Open the Now Mobile app.
   b. Select **Help center**.
   c. Under Browse all topics, select **Industrial Services**.
   d. Follow the same steps as you would in the desktop experience above to submit the request or save it as a draft.

Result

When you report the OT incident, an overview of the incident is provided along with a link in the activity stream to view the incident in the Industrial Workspace.

Note: When you view the incident in the Industrial Workspace, you have read-only access and cannot edit the record fields. You can only add comments or work notes.

You can also view your request in the Employee Center by selecting **My Requests**. Viewing your request on the requests page lets you see any work notes or activities saved to your submitted request.

Industrial Workspace

The Industrial Workspace is a user interface that provides Operational Technology (OT) users with the tools they need to manage their OT data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Explore	Configure	Use
		
Exploring the Industrial Workspace	Plan and configure your implementation	Using the Industrial Workspace

Exploring the Industrial Workspace

The Industrial Workspace is a user interface that provides Operational Technology (OT) users with the tools they need to manage their OT data.

Industrial Workspace navigation

The Industrial Workspace is organized into the following pages.

Industrial Workspace pages

Page	Description
OT Action-Oriented Landing Page	When you select the **Home** ( ) icon, you're taken to the OT Action-Oriented Landing Page. The landing page helps you keep track of critical tasks related to your OT network.
Dashboard Library	When you select the **Dashboard Library** ( ) icon, you're taken to the dashboard library that contains the following dashboards. **OT Visibility dashboard** Contains the data related to your OT devices. **Operational Technology Vulnerability Response (PA) dashboard** Tracks the volume, performance, and progress of the OT vulnerable items from the initial analysis and detection to the containment, or remediation. **OT Vulnerability Risk Rollup dashboard** Contains the risk score of the OT devices at each level of the equipment model.
OT Progress Scorecard	When you select the **OT Progress Scorecard** ( ) icon, you're taken to the OT Progress Scorecard. The OT Progress Scorecard lets you compare site data in one view.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Industrial Workspace pages (continued)

Page	Description
Industrial Workspace list view	When you select the **List** () icon, you're taken to the Industrial Workspace list view, which gives you access to all the lists related to your OT data records. You can access the following list modules and their subsequent lists: • Operational Technology (OT) • Information Technology (IT) Hardware • Industrial Process Manager • OT Incidents • OT Change Requests • OT Remediation Tasks • OT Vulnerable Items • OT Tasks • Knowledge
Equipment Model Manager	When you select the **Equipment Model** icon,  , you're taken to the Equipment Model Manager, where you can view your sites and their equipment model data.

Operational Technology Action-Oriented Landing Page

You can use the Operational Technology (OT) Action-Oriented Landing Page to track critical tasks related to your OT network.

OT Action-Oriented Landing Page overview

The OT Action-Oriented Landing Page helps users, such as OT engineers, view tasks assigned to them, their site, or their group. The landing page calls out important actions that must be prioritized for the signed-in user and includes an overview of existing OT incidents, OT change requests, OT remediation tasks, OT vulnerable items, and other tasks.

The landing page provides a detailed and role-based view of the daily tasks and important actions. Each task in the **Important Action** section shows tasks sorted by their **Opened** date by default. If the task is critical, then it shows up in the **Important Action** section.

To access the OT Action-Oriented Landing Page, navigate to **All** > **Industrial Workspace**, select the Home () icon.

Landing page contents

The following sections describe the content that you can view in the OT Action-Oriented Landing Page.

Important actions

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Important actions section contains OT tasks or actions that are considered critical and must be addressed as soon as possible. By default, the tasks are organized by their **Opened** date with the most recently created critical task assigned to the signed in user shown first.

The tasks shown in this section are the most critical tasks pulled from the **Overview** section that you can act on. Task criticality is determined by the following criteria:

- Their priority is critical
- The task is a remediation task and its risk rating is critical

The tasks included in this section are organized in the following ways:

- All tasks directly assigned to the signed in user are shown first.
- Tasks assigned to a user's group that are also not assigned to any user are shown after.
- Tasks that aren't assigned to a group or user but are assigned to a site the signed in user has access to are shown last.

Overview

The Overview section contains an overview of OT incidents, change requests, remediation tasks, vulnerable items, and other tasks assigned to you, your group, or your site.

You can use the following filters to view the records shown based on the **Assigned to**, **Assignment group**, and **Site** fields on the records:

Your work

Records assigned to you.

Your group's work

Records assigned to your group or groups.

Your site's work

Records assigned to your site or sites.

The following table describes the tiles in the Overview section.

Overview tiles

Tile	Description
OT Incidents assigned to you / OT Incidents assigned to your groups / OT Incidents assigned to your sites	Number of OT incident records assigned to either you, your assignment group, or your site. To view a list of all the OT incident records, select **All records**. To only show the list of records based on their state or type, select the respective section of the available graph. For example, if you only want to view the incident records based on their priority, select the **Critical** section of the graph.
OT Change Requests assigned to you / OT Change Requests assigned to your groups / OT Change Requests assigned to your sites	Number of OT change request records assigned to either you, your assignment group, or your site. To view a list of all the OT change request records, select **All records**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview tiles (continued)

Tile	Description
	To only show the list of records based on their state, select the respective section of the available graph. For example, if you only want to view the change request records that are scheduled, select the **Scheduled** section of the graph.
OT Remediation Tasks assigned to you / OT Remediation Tasks assigned to your groups / OT Remediation Tasks assigned to your sites	Number of OT remediation task records assigned to either you, your assignment group, or your site. To view a list of all the OT remediation task records, select **All records**. To only show the list of records based on their state, select the respective section of the available graph. For example, if you only want to view the remediation task records that are in review, select the **In Review** section of the graph.
OT Vulnerable Items assigned to you / OT Vulnerable Items assigned to your groups / OT Vulnerable Items assigned to your sites	Number of OT vulnerable item records assigned to either you, your assignment group, or your site. To view a list of all the OT vulnerable item records, select **All records**. To only show the list of records based on their risk rating, select the respective section of the available graph. For example, if you only want to view the vulnerable item records that are a high priority, select the **High** section of the graph.
Other OT Tasks assigned to you / Other OT Tasks assigned to your groups / Other OT Tasks assigned to your sites	Number of other OT task records assigned to either you, your assignment group, or your site. To view a list of all the other OT task records, select **All records**. To only show the list of records based on their priority, select the respective section of the available graph. For example, if you only want to view the OT tasks that are considered low priority, select the low section of the graph.

OT *CMDB* Health

The OT *CMDB* Health helps you monitor and maintain the health of your devices in the Configuration Management Database (CMDB). You can view the number of your OT devices organized by type.

Note: This section is only displayed if you have Operational Technology Manager installed.

The following table describes the tiles in the OT *CMDB* Health section. To view the OT *CMDB* Health section, you must have the **cmdb_ot_isa_viewer** role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT CMDB Health tiles

Tile	Description
Unclassed OT devices	Number of the OT devices in your OT network that aren't assigned an OT device type category. To view the list of unclassed OT device records, select **All records**.
Unassigned OT devices	Number of the OT devices in your OT network that aren't assigned to a user. To view the list of unassigned OT device records, select **All records**.
Unmapped OT devices	Number of the OT devices in your OT network that aren’t mapped to any equipment model entity for your assigned site. To view the list of unmapped OT device records, select **All records**. **Note:** This tile is only available when the Industrial Process Manager is installed and if the signed in user has the cmdb_ot_isa_viewer role. The tile requires that your organization has an equipment model for mapping OT devices to a production process.
No site assigned	Number of OT devices in your OT network that aren't assigned to a site. **Note:** This tile is only available if the signed in user has the cmdb_ot_isa_viewer role. To view the list of OT device records without a site, select **All records**.
No IP address OT devices	Number of OT devices in your OT network that aren't assigned an IP address. To view the list of OT device records without an IP address, select **All records**.

Dashboard Library in the Industrial Workspace

The Dashboard Library in the Industrial Workspace contains the Operational Technology Visibility dashboard, the Operational Technology Vulnerability Response (PA) dashboard, and the Operational Technology Vulnerability Risk Rollup dashboard.

Operational Technology Visibility dashboard

The Operational Technology (OT) Visibility dashboard helps you manage your OT device in a centralized location. The OT Visibility dashboard lets you the access your OT device data.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Visibility dashboard overview

The OT Visibility dashboard is a centralized location in the Industrial Workspace. You can use this dashboard to review your Operational Technology Manager and Industrial Process Manager data. You can also use it to review or edit the detailed information for the OT devices and equipment model entities in your OT network.

With the OT Visibility dashboard, you can achieve the following:

- Understand what OT device information changed in your OT network in the past week.
- View the progress of an OT device inventory through an industrial facility.
- Analyze your OT devices in meaningful ways. For example, you can gain insights into how many of your production devices map to your production processes.

Dashboard contents

To access the OT device data in the OT Visibility dashboard, navigate to **All** > **Industrial Workspace**, select the Dashboard Library () icon, and then select the **Operational Technology Visibility**. To access the key performance indicators (KPI) graph for any tile that is described in the following table, select the number count or chart component in the tile.

The following table describes the OT device data that you can see on the different tiles on the dashboard.

Dashboard tiles

Tile	Description
Updates from the past 7 days	
New OT devices discovered	Number of the new OT devices that were discovered by Discovery for Operational Technology and other automated processes in your OT network during the last seven calendar days.
Inactive OT devices	Number of the OT devices that haven't appeared in your OT network during the last seven calendar days. These devices are considered inactive.
OT devices overview	
Total CMDB OT devices	Number of the OT devices in your OT network.
Unclassed OT devices	Number of the OT devices in your OT network that aren't assigned with an OT device type category.
Unassigned OT devices	Number of the OT devices in your OT network that aren't assigned to a user.
Unmapped OT devices	Number of the OT devices in your OT network that are not mapped to any equipment model entity for your assigned site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Dashboard tiles (continued)

Tile	Description
	Note: This tile is only available when the Industrial Process Manager is installed because it requires that your organization has an equipment model for mapping OT devices to a production process.
OT devices by category	
Supervisory systems	Number of the OT devices in your OT network that are assigned to a Supervisory systems category.
Control systems	Number of the OT devices in your OT network that are assigned to the Control systems category. **Note:** Control modules aren't included in this number.
Field devices	Number of the OT devices in your OT network that are assigned to the Field devices category.
Computers and servers	Number of the OT devices in your OT network that are assigned to the Computers and servers category.
Network Gear	Number of the OT devices in your OT network that are assigned to the Network Gear category.
Industrial IoT	Number of the OT devices in your OT network that are assigned to the Industrial Internet of Things (IoT) category.
OT devices by Purdue level	Bar chart that indicates the number of OT devices in your OT network by their assigned Purdue level. **Note:** To learn more about the Purdue levels in the OT systems, see https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.
OT devices by type (Top Level)	Bar chart that categorizes the OT device data by the OT device types.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Dashboard tiles (continued)

Tile	Description
OT devices by manufacturer (Top Level)	Pie chart that indicates the number of OT devices in your OT network by their assigned manufacturer.
OT devices by criticality	Pie chart that indicates the number of OT devices in your OT network by their assigned criticality.

Required roles to view the dashboard

To access the OT Visibility dashboard, you must have the **cmdb_ot_viewer** and **cmdb_ot_isa_viewer** roles.

Site filter

You can use the **Site** filter to search for and select the site that you want to view on the dashboard. To access and use the site filter, you must have the **cmdb_ot_isa_viewer** role with access to the site you want to view.

For more information, see Use the site filter.

Operational Technology Vulnerability Response (PA) dashboard

Track the volume, performance, and progress of the Operational Technology (OT) vulnerable items (VIs) from the initial analysis and detection to the containment, or remediation. You can filter the reports by the assignment group, exploits, risk rating, or state to get insight into your vulnerability exposure and the services that are affected.

Required Operational Technology and Operational Technology Vulnerability Response roles

To access the OTVR (PA) dashboard, you must have the **sn_otvr.remediation_owner** role.

To view the Operational Technology Vulnerability Response (PA) dashboard, navigate to **All** > **Industrial Workspace** and select the **Dashboard Library** () icon in the navigation panel. Then select **Operational Technology Vulnerability Response**.

Use cases

The following table shows some examples of how different people in your organization can use this dashboard.

Operational Technology Vulnerability Response (PA) dashboard use cases

User	Dashboard use
OT site managers, OT analysts, vulnerability remediation owners	Help your organization deal with increasing security incidents due to exploited vulnerabilities by determining which OT vulnerable items present the most risk. This dashboard provides a graphical view into the OT vulnerable item activity and can help you to design the remediation plans

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Vulnerability Response (PA) dashboard use cases (continued)

User	Dashboard use
	and status progress. You can focus on the key performance indicators (KPIs) that are associated with the critical affected devices and high-visibility vulnerabilities.

Dashboard tabs

You can see the reports that show the trending data over time and the reports with real-time data. You can also view the trends of the important metrics on a regular schedule. This enables you to analyze your overall business processes and identify the areas that require improvement.

Learn what's in the **Vulnerable Items** tab, **Remediation** tab, and **Exceptions** tab.

Vulnerable Items tab

The **Vulnerable Items** tab communicates the KPIs for the vulnerability risk and prevalence, affected devices, remediation target adherence, and remediation progress.

On the **Vulnerable Items** tab, you can view the following reports:

- Total OT Vulnerable Items
- New OT Vulnerable Items
- OT Unassigned Vulnerable Items
- OT Vulnerable Items by State
- OT Vulnerable Items by Risk Rating
- OT VIs Met Remediation Target

  Note: You can view the data by the last month, 3 months, 6 months, year, or all time.

- OT VI Mean Time to Remediate (MTTR)

  Note: You can view the data by the last month, 3 months, 6 months, year, or all time.

- OT VI by age
- OT Closed Vulnerable Items by Remediation Target Status
- OT Critical Vulnerable Items by Assignment Group
- OT Overdue Critical Vulnerable Items by Assignment Group

Remediation tab

The **Remediation** tab helps you to understand the progress of your remediation actions and to see which support teams need the most assistance with their completion.

On the **Remediation** tab, you can view the following reports in real time:

- OT Remediation Tasks
- OT Critical Remediation Tasks Near Due
- OT Remediation Task by Risk Rating
- OT Remediation by Target Status

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- OT Remediation Task by State
- OT Unassigned Remediation Tasks
- OT Critical Remediation Task by Assignment Group
- OT Overdue Critical Remediation Task by Assignment Group

Exception tab

The **Exception** tab helps you to understand where your organization is taking a risk due to potentially excessive deferrals of remediation.

On the **Exception** tab, you can view the following reports in real time:

- OT Deferred Vulnerable Items by Reason
- OT Exceptions for Critical Vulnerable Items by Assignment Group.

Site filter

You can use the **Site** filter to search for and select the site that you want to view on the dashboard. To access and use the site filter, you must have the **cmdb_ot_isa_viewer** role with access to the site you want to view.

For more information, see Use the site filter.

Indicator sources

The Operational Technology Vulnerability Response indicators gather data from the following sources:

- OTVI.Active
- OTVI.Closed
- OTRT.Active

For more information about the indicator sources that are used for the dashboard, see Indicator sources and indicators for the Operational Technology Vulnerability Response (PA) dashboard.

If the expected number of records from the indicator sources exceeds 1 million, you must override the expected count in the Records collection section of the indicator source. For more information, see Review the indicator sources for a larger number of records.

Indicators

Several indicators are used to measure and track the progress of your vulnerability remediation in the Operational Technology Vulnerability Response application. For more information about the indicators used for the dashboard, see Indicator sources and indicators for the Operational Technology Vulnerability Response (PA) dashboard.

The **collect records** option for the indicators is inactive by default for the Operational Technology Vulnerability Response application. This option is turned off to avoid the performance issues that may occur when you collect a large amount of data for each indicator.

Breakdowns

Breakdowns filter and group the collected records by a qualitative attribute. The following breakdowns apply to the indicators on the dashboard:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Age
- Age Closed
- Assignment Group
- CI Manager
- Deferral Reason
- Exploit Attack Vector
- Exploit Exists
- Exploit Skill Level
- Remediation Target Rule
- Remediation Target Status
- Remediation Target Status (Closed)
- Risk Rating
- Severity
- State

The breakdown sources specify the unique values that a breakdown contains. The unique values are called the breakdown elements. The dashboard uses the following breakdown sources:

- Assignment Group
- Deferred.Reason.Non.Closed
- Exploit Attack Vector
- Exploit Exists
- Exploit Skill Level
- OT Age Range
- Remediation Target Status
- Remediation Target Status (Closed)
- Remediation.Target.Rule
- Risk Rating
- Severity
- State
- Vulnerable.Item.CI.Manager

For more information about the breakdowns and breakdown sources, see Operational Technology Vulnerability Response (PA) dashboard breakdowns.

Collection jobs

The dashboard uses the following collection jobs to gather the OT vulnerability data that are displayed on the dashboard.

- [PA OT VR] Historical Vulnerability Data Collection
- [PA OT VR] Daily Collection for Remediation Tasks
- [PA OT VR] Daily Collection for Vulnerable Items 1
- [PA OT VR] Daily Collection for Vulnerable Items 2

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information about the collection jobs, see Operational Technology Vulnerability Response (PA) dashboard collection jobs.

Data visualizations

The Operational Technology Vulnerability Response (PA) dashboard uses data visualizations to display your OT vulnerability data. For example, the total number of OT vulnerable items in your system is displayed in the **Total OT Vulnerable Items** bar chart and is grouped by OT device type.

For more information about the data visualizations that are used in the dashboard, see Data visualizations used in the Operational Technology Vulnerability Response (PA) dashboard.

Operational Technology Risk Management dashboard

The Operational Technology (OT) Risk Management dashboard contains the risk score and the vulnerability items (VITs) of the OT devices at each level of the equipment model.

About OT Risk Management dashboard

The OT Risk Management dashboard is available in the Dashboard Library ( ) of the Industrial Workspace. The following tables are available for your rolled up vulnerability risk scores in the OT Risk Management dashboard:

- Vulnerability risk table for your equipment model entities
- Vulnerability risk table for OT devices with no site assigned

OT Risk Management dashboard tables

Table	Description
Vulnerability risk table for your equipment model entities	Displays the risk scores for your site's equipment model entities and their VITs. It also highlights the area that poses the most risk and the number of VITs.
Vulnerability risk table for no site assigned OT devices	Displays the risk scores and count of vulnerable items for OT devices that aren't assigned to any site

You can view all the VIT records created for an entity by selecting the displayed number of VITs. Additionally, you can select a VIT record and view its details.

Required roles to view the dashboard

To access the OT Risk Management dashboard, you must have the **sn_otvr.remediation_owner**, **cmdb_ot_isa_viewer**, and the **admin** role.

View OT Vulnerability Risk of a site

You can use the Site list to search for and select the site that you want to view on the dashboard.

Select the **OT Vulnerability Risk** from the Select Risk Type list to view the rolled up risk score and the VITs for the selected sites.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Progress Scorecard

The Operational Technology (OT) Progress Scorecard lets you compare device and vulnerable item data between your sites.

OT Progress Scorecard overview

The OT Progress Scorecard is a centralized location in the Industrial Workspace that lets you compare your site data. Site data includes both OT device data and vulnerability data. With the OT Progress Scorecard, you can track site progress and determine the sites that need attention.

You can also view the site data for the following Operational Technology applications:

- Operational Technology Manager
- Operational Technology Vulnerability Response
- Operational Technology Incident Management
- Operational Technology Change Management

You can configure the OT Progress Scorecard using the Industrial Workspace Admin Guided Setup. For more information about the setup tasks, see Setting up the Operational Technology Progress Scorecard.

Scorecard contents

To access the OT Progress Scorecard, navigate to **All** > **Industrial Workspace** and select the **OT Progress Scorecard** ( ) icon.

The following table describes columns in the OT Progress Scorecard.

OT Progress Scorecard columns

Column	Description
Overall Score (%)	The progress of your site determined by the indicators on the scorecard. You can edit the weightage to control how much an indicator contributes to the overall score. For more information, see Set the system properties for the Operational Technology Progress Scorecard.
% of Expected OT Devices in CMDB	The percentage of your OT devices that you expect to have in the Configuration Management Database (CMDB). **Note:** If you see a value of -1, then one or more of the values in the % of Expected OT Devices in CMDB indicator is missing the **Expected OT Device** attribute in the OTPSC Attributes table. For information about how to configure expected OT devices see Configure the expected OT devices for a site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Progress Scorecard columns (continued)

Column	Description
Classified OT Devices (%)	The percentage of classed OT devices. Classified OT Devices (%) doesn't include OT devices classed as cmdb_ci_ot.
Assigned OT Devices (%)	The percentage of OT devices with values in the following fields: • Assigned to • Owned by • Managed by • Supported by • Approval group • Managed group • Support by • Change group
OT Device Data Completeness (%)	The percentage of OT devices that meet your data goals. This metric depends on the CMDB Health Dashboard - Completeness Score Calculation job and you must set the required & recommended fields on the CI Class Manager. For more information, see Configuring CMDB Health. Completeness is a KPI determined by the following metrics: **Required** Measures the percentage of CIs in which fields that are defined as required, aren't populated. Missing fields are tagged as incomplete noting that for this CI some information is missing. **Recommended** Measures the percentage of CIs in which fields that are set as recommended, aren't populated. For more information about data completeness, see CMDB Health KPIs and metrics. **Note:** If you see a value of -1, then the CMDB Health Dashboard - Completeness Score Calculation job hasn't been run yet. Or the job has been run with an incomplete status.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Progress Scorecard columns (continued)

Column	Description
Mapped OT Devices (%)	The percentage of OT devices mapped to an equipment model entity. **Note:** If you see a value of 0, then no OT devices have been found.
Backed up OT Devices (%)	The percentage of OT devices with backup records created. **Note:** If you see a value of 0, then no OT devices have been found.
Assigned OT Vulnerable Items (%)	The percentage of OT vulnerable items that aren't closed and addressed. **Note:** If you see a value of 0, then no OT devices have been found.
Approved OT Change Requests (%)	The percentage of OT change requests that are submitted and approved. **Note:** If you see a value of 0, then no OT devices have been found.
OT Incidents with OT Context (%)	The percentage of OT incidents that have OT device or equipment model data. **Note:** If you see a value of 0, then no OT devices have been found.

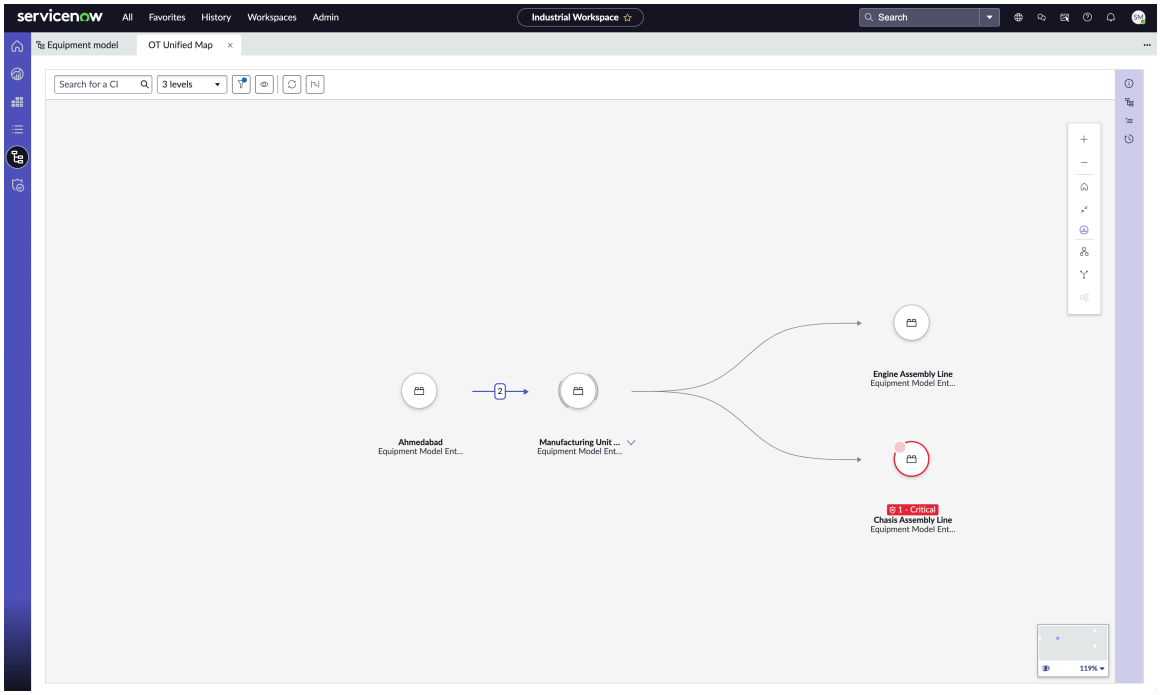
Operational Technology Unified Map experience in the Industrial Workspace

The Operational Technology (OT) Unified Map available in the Industrial Workspace provides a unified experience to view the relationships between devices and other configuration items (CIs), and view related items, like OT incidents and change requests.

Unified Map overview

The OT Unified Map experience shows a hierarchical map of CIs and their relationships while centered on a selected CI, known as a home node. The experience combines the capabilities of dependency views and service mapping into a single map experience. The following image shows an example of what the OT Unified Map experience looks like in the Industrial Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



You can access a Unified Map in the following locations in the Industrial Workspace.

- ISA record in the Equipment Model Manager
- OT incident record
- OT change record

The side panel of the Unified Map lets you view additional information related to the map by selecting the following icons.

Unified Map panel icons

Icon	Description
Attributes	Details of the selected node on the map, including the following attributes: • Class • Location • Owned by • Updated • Discovery source • Most recent discovery • Business contact • Life Cycle stage • Operational status • Service classification • Service portfolio • Severity

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Unified Map panel icons (continued)

Icon	Description
	• Traffic based discovery • Version
Application services	Equipment model entities or devices that comprise the application service.
Related items	Other records related to the selected node. The related items include: • Past OT Changes • Current OT Changes • Planned OT Changes • Active OT Incidents • Active OT Alerts • OT Vulnerable Items
Changes 	History of changes made to the Unified Map.

For more information about configuring the OT Unified Maps experience, see Setting up the Operational Technology Unified Map experience.

For more information about viewing an OT Unified Map, see View an Operational Technology Unified Map.

Operational Technology Hardware Vulnerability Assessment

The Operational Technology (OT) Hardware Vulnerability Assessment (HVA) application enables you to assess the firmware vulnerabilities of the OT devices in inventory and create vulnerable items (VIT) against the impacted OT devices.

Hardware Vulnerability Assessment overview

Hardware Vulnerability Assessment uses normalized content for firmware discovery model to perform assessments. The normalized content contains OT device data, such as manufacturer, firmware version, and product model. It's based on the normalization process available in Enterprise Asset Management. The normalized content for OT devices is mapped according to the Common Platform Enumeration (CPE) format provided by the National Vulnerability Database (NVD). An OT device is considered at risk, when the Common Vulnerabilities and Exposures (CVEs) data available in the NVD database, matches the OT device data available in the CPE-mapped normalized content. The Hardware Vulnerability Assessment menu available in the Industrial Workspace displays the OT devices that are at risk.

HVA can assess firmware discovery models, which don’t have normalized content and they haven’t been CPE-mapped yet. HVA uses a matching score algorithm to compare CPE values with existing firmware discovery values. The matching algorithm searches for CPEs that matches OT devices with the same discovery publisher name, model name, and version. The HVA matching algorithm compares the data from CPEs and unmapped firmware discovery model. Based on the comparison, the matching algorithm evaluates the best possible CPE match for unmapped firmware discovery models. Even though the results may not be fully accurate, it helps in vulnerability assessments until CPE-mapped normalized content is available.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Also, HVA uses the range information provided by NVD to assess vulnerabilities more accurately. For example:

- In case there's a version information unavailable for a CPE, the range information available for a specific OT device publisher and model is used to perform a hardware vulnerability assessment.
- For versions, a comparison algorithm is used to determine if the input version is in range.

Important: If you're already using HVA, rerun the NVD Integrations to use the range information feature. For more information, see Run NVD Integrations for Hardware Vulnerability Assessment.

You must activate and schedule the following scheduled jobs to perform hardware vulnerability assessment automatically and periodically:

- *Hardware Vulnerability Assessment - Full*
- *Hardware Vulnerability Assessment - Delta*

Required Operational Technology and Hardware Vulnerability Assessment roles

You must have the following roles to use the Hardware Vulnerability Assessment (HVA) menu:

- sn_vul.manage_exposure_assessment: Assign roles to admin users or user groups as needed, which enables them to view or edit properties for HVA.
- sn_otvr.vul_event_manager (OT Vulnerability Event Manager): Assign roles to HVA users or user groups as needed, which enables them to view assessment records and act accordingly.

Use Case

OT hardware vulnerability analysts can use HVA to:

- Identify cybersecurity risks in OT devices.
- Focus on high-risk vulnerabilities via fully matched assessments on OT device data.
- Set up automatic creation of vulnerable items for fully matched assessments.
- Investigate and address partially matched assessments to identify potential risks and act accordingly.
- Monitor unprocessed OT devices from the **Awaiting Normalization** tab, which are pending full discovery or pending content updates.

HVA tabs

The HVA menu displays HVA records created for the OT devices. These assessment records are created based on many criteria. For example, CVE vulnerability, OT device at risk, Common Vulnerability Scoring System (CVSS) score, Confidence Score, and Device Criticality.

- The **Fully matched assessments** tab displays the assessment records, where the CVEs fully match with the manufacturer, product model, and firmware version of the OT devices. A fully matched assessment means that an OT device matches all vulnerability factors specified in a CVE.
- The **Partially matched assessments** tab displays the assessment records, where the CVEs partially match the firmware version or the manufacturer and model on the OT device. Also, HVA creates partial assessments for normalized discovery models, which don't have firmware version available. Using the matching algorithm, the version information from the normalized content of OT devices with the same publisher and model is used to create an assessment.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The **Vulnerable Items** tab displays the VITs that are created automatically or you create manually based on the assessments.
- The **Ignored assessments** tab displays the assessments of the devices that you choose to ignore.
- The **Awaiting Normalization** tab displays the OT device data that doesn't have the normalized data and hasn't been used for assessment.

Important:

- If the property to create automatic VIT is enabled, the **Fully matched assessments** tab doesn't display any data. You can view this information on the **Vulnerable Items** tab.
- Enable the Firmware Discovery Model Opt-in feature in Enterprise Asset Management so that OT devices data are available for normalization. For more information, see Opt-in to the Enterprise Asset Management Content Service.

Additional Resources

Related topics

Enterprise Asset Management normalization

Industrial Workspace

Set up the Hardware Vulnerability Assessment of Operational Technology devices using guided setup

Use the Hardware Vulnerability Assessment menu in the Industrial Workspace

Confidence score calculation for hardware vulnerability assessment

Confidence Score is displayed for partially matched assessments, vulnerable items (VITs), and ignored assessments.

About Confidence Score Calculation

HVA uses a scoring mechanism called Confidence Score to indicate the accuracy of the CVE data matching the CPE-mapped normalized content of an OT device. Confidence Score is an aggregated calculation of the matching scores created by the matching algorithm in HVA.

The Confidence Score varies for the following assessments:

- Fully matched assessments: The Confidence Score is 1 for full assessments as all the parameters in the CVE information matches the device discovery model values available for the OT device.
- Partially matched assessments: The Confidence Score is less than 1 for partial assessments as all the parameters in the CPE information doesn't match the device discovery model values available for the OT device.

How to calculate the confidence score

If you compare the samples of the CPE Firmware mapped to the OT device and the discovery model for the OT device, you can see that:

- There is only a partial match for the **Model** information. Due to a partial match, the model score is assigned a value of 20.
- The **Version** information doesn't match so the version score is assigned a value of 0.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The confidence score range is 0–1. Based on the CPE information, the confidence score is calculated using the following formula:

```
((BASE SCORE) + (publisher score) + (model score) + (version
 score)) / 100
```

=

```
((25) + (25) + (20) + (0)) / 100
```

=

```
70 / 100
```

=

```
.70
```

Note: To refer to the values used to calculate the confidence score, see Confidence score reference tables for hardware vulnerability assessment.

Confidence score reference tables for hardware vulnerability assessment

Reference values used to calculate the confidence score.

Reference tables

Confidence score calculation reference table

Information available in discovery model for OT device	Information available in CPE mapped to OT device	Partial match score	Additional score for full match
Discovered Publisher name	Publisher	20	5
Discovered Model name	Model	20	5
Discovered Version	Version	0	25

Confidence score summary table

Score	Value
Sum of all scores	75
Base score **Note:** Minimum score given to all matched discovery models.	25
Total score	100

Operational Technology Network Map

The Operational Technology (OT) Network Map is an interactive map that visualizes your OT network through connected nodes.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

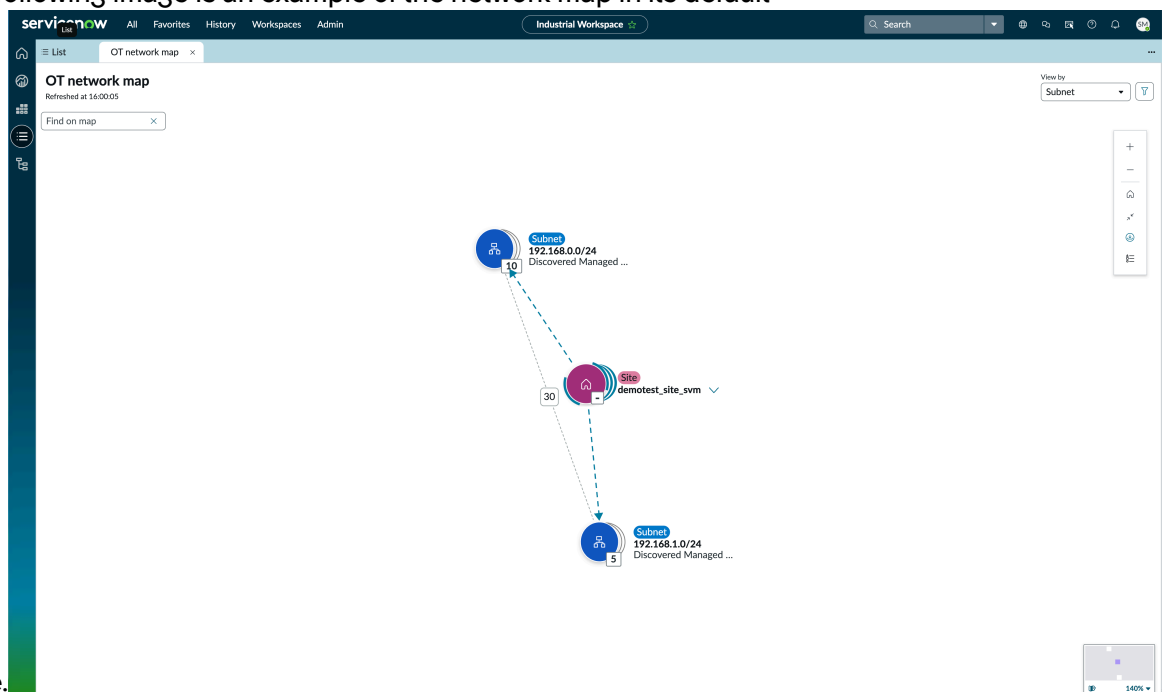
OT Network Map overview

The OT Network Map provides a real-time and accurate representation of your OT environment by modeling subnets and device-to-device connections across your industrial network. This visual map helps you understand how OT devices are connected and how data flows between them.

With this visibility, you can analyze the impact of network changes, identify connectivity risks, and make informed operational and security decisions. It enables faster troubleshooting, improves risk awareness, and provides better visibility into complex OT network relationships. It helps you move from reactive troubleshooting to proactive decision-making across your industrial environment.

You can access the OT Network Map by navigating to Equipment Model Manager in the Industrial Workspace and selecting a site.

The following image is an example of the network map in its default state.



Node map representation

The node at the center of the network map represents your equipment model entity site. Connected to the site, you can see the nodes that represent the site's subnets. On each subnet node, there's a number indicating how many OT devices exist within that subnet. When you select the device number on the subnet node, the network map expands to show all the device nodes within the subnet.

Subnet node details

When you hover over the subnet node, you can view the following information for that subnet:

- Subnet name
- Number of critical devices
- Total number of OT devices
- Managed Network name, if available

Device node details

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you hover over the device node, you can view the following information for that device:

- Device name
- Device type
- Criticality status

The device node also contains an option to view its device-to-device connections. For more information about device-to-device connections, see OT device related items and related lists and View and edit device to device connections.

Map refresh

When the **OT Network Map Cache Handler** scheduled job runs and the **Refreshed at** field in the map is updated with the new refresh time. For more information about the scheduled job, see Run the OT Network Map Cache Handler scheduled job.

Populating the map

To populate the OT Network Map, you must run the **OT Network Map Cache Handler** scheduled job. For more information about the scheduled job, see Run the OT Network Map Cache Handler scheduled job.

The data must be available in the following tables for the network map to load properly.

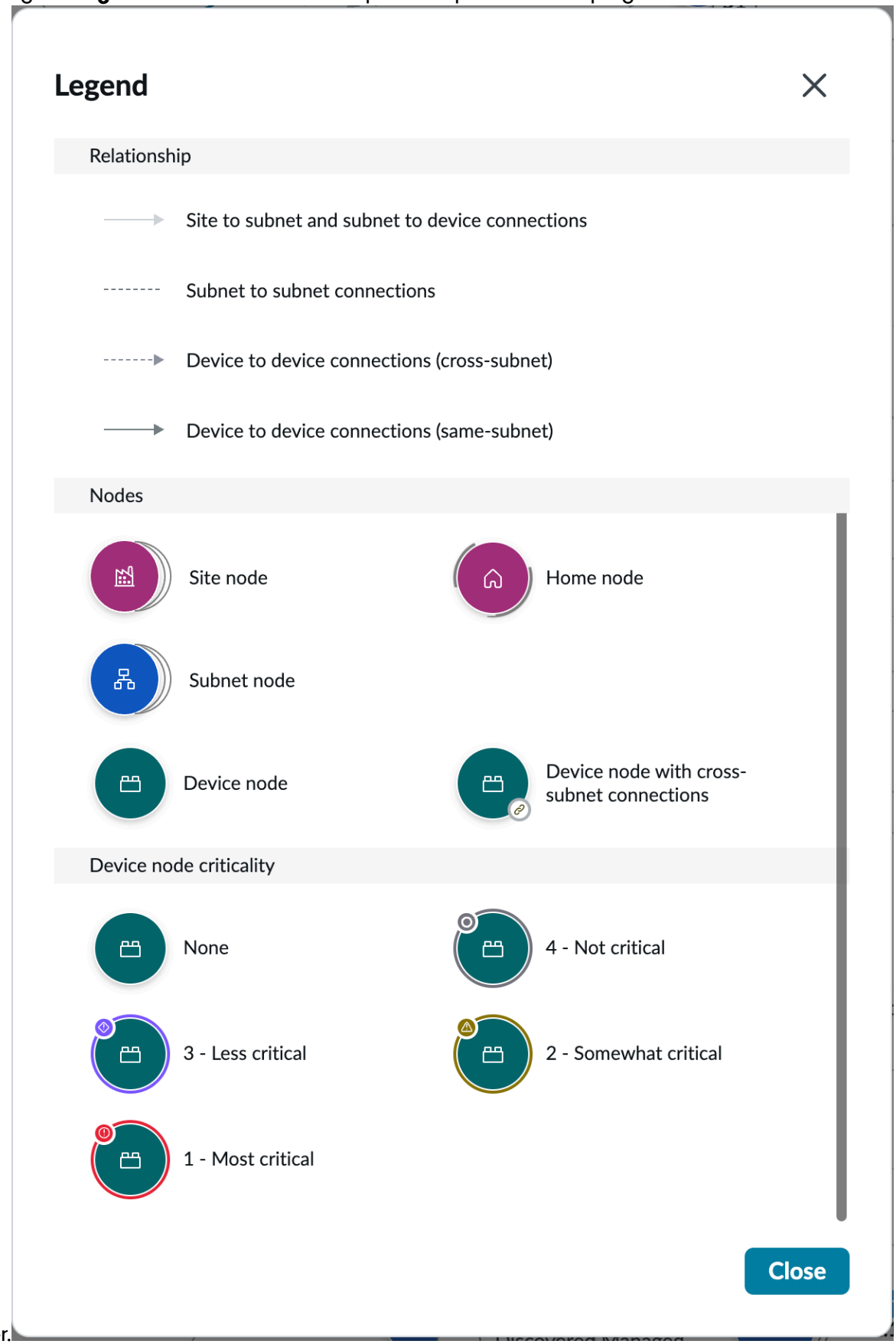
- IP Address [cmdb_ci_ip_address]
- OT Discovered Subnet [sn_ot_discovered_subnet]

Map legend

The OT Network Map contains a legend that describes the visual components of the map and their meaning. The legend covers the relationship lines between nodes, the different nodes you may see in your network, and the device node criticality. The following image shows the map legend made available by

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

selecting the **Legend** icon from node map control panel in the top-right corner.



© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Map filters

The following table contains the additional filters that you can apply to the OT Network Map for your equipment model entity.

OT Network Map filters

Filter	Description
Class	The name of the assigned class for the OT device.
Criticality	The measure of the relative risk to the site process due to failure of the device.
Manufacturer	The device manufacturer.
Purdue level	The assigned Purdue level. Ranges 0–5.
Discovery source	The Discovery source for the OT device data.

Roles required

You must be assigned both the **cmdb_ot_isa_viewer** role and **cmdb_ot_viewer** role.

Limitations of the network map

The following list contains the limitations of the network map.

- Subnets without any configuration items (CIs) don't show up in the network map.
- CIs that aren’t part of any subnet don't show up in the network map.
- For a site with more than 10K CIs, only 10K CIs are considered in the OT network map calculations.

What to do next

- Setting up the OT Network Map
  - Run the OT Network Map Cache Handler scheduled job
  - Set the system property for the OT Network Map
- View and edit the OT Network Map

Configuring the Industrial Workspace

Configure Industrial Workspace so that you can manage your Operational Technology (OT) data.

If you have the admin role, you can use Guided Setup to lead you through the setup of the Industrial Workspace. Guided Setup is a tool that assists with application or capability configuration. It organizes the configuration activities into categories. These categories contain the information about the setup tasks, the steps to complete each task, and links to the pages in your instance where you perform the configuration. The links to useful help content are also provided.

To access Guided Setup, navigate to **Industrial Workspace Admin** > **Guided Setup**.

The following table lists the Guided Setup tasks and their purposes for the Industrial Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Industrial Workspace setup tasks

Task	Purpose
Assign the Industrial Workspace role.	Assigns the Configure Industrial Workspace [configure_industrial_workspace] role to users that need to configure the Industrial Workspace.
Review the homepage destination rules.	Redirects users to different pages in the Industrial Workspace based on user criteria.
Complete the configuration tasks for the OT Action-Oriented Landing Page.	Configures the OT Action-Oriented Landing Page so users can access the landing page in the Industrial Workspace.
Complete the configuration tasks for the OT Progress Scorecard.	Configures the OT Progress Scorecard so users can begin comparing site data and progress in the Industrial Workspace.
Complete the configuration tasks for the OT Visibility dashboard.	Configures the tabs on the OT Visibility dashboard so users can access the dashboard in the Industrial Workspace.
Complete the configuration tasks for the Operational Technology Vulnerability Response (PA) dashboard.	Configures the Operational Technology Vulnerability Response (PA) dashboard in the Industrial Workspace.
Complete the configuration tasks for the OT Unified Map experience	Configures the OT Unified Map experience if you want to modify the default settings.

Assign the Industrial Workspace role

Assign the Industrial Workspace role to your users so that you can control their access to the workspace's features, capabilities, and data.

Before you begin

Role required: admin

About this task

Users with the role that are listed in the following table can access the Guided Setup for the OT Action-Oriented Landing Page and the OT Progress Scorecard.

OT Progress Scorecard role

Role	Description
Configure Industrial Workspace [configure_industrial_workspace]	Can access the Industrial Workspace and the Guided Setup for the OT Action-Oriented Landing Page and the OT Progress Scorecard.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Review the homepage destination rules for the Industrial Workspace

Review the homepage destination rules for the Industrial Workspace.

Before you begin

Role required: configure_industrial_workspace

About this task

The homepage destination rules redirect users to different pages in the Industrial Workspace based on user criteria. For more information about the homepage destination rules, see Industrial Workspace homepage destination rules.

Procedure

1. Navigate to **All**.
2. In the **Filter** field, add `sys_homepage_destination_rule.list`.
3. Press the Enter key.
4. Select one of the following Industrial Workspace homepage destination rules whose user criteria you want to edit:
   - OT Progress Scorecard Page
   - Industrial Workspace Home Page
   - OT Dashboard Library Page

     Note: The OT Dashboard Library Page rule only displays if Operational Technology Manager is installed.

   - ISA Equipment Model Page

     Note: The ISA Equipment Model Page rule only displays if Industrial Process Manager is installed.

   - Industrial Workspace List Page
5. In the **User Criteria** field, copy the user criteria.
6. To apply the user criteria that redirects users to the page in the Industrial Workspace that you select, complete the following steps.
   a. Navigate to **All** > **User Criteria**.
   b. In the list view's search bar, search the homepage destination rule's user criteria you copied in step 5.
   c. Modify the User Criteria record so that the required users that you want redirected match the user criteria.
   d. Select **Update**.

Result

The users, groups, and roles defined in the user criteria record are now automatically redirected to the selected page in the Industrial Workspace.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setting up the Operational Technology Action-Oriented Landing Page

Set up the Operational Technology (OT) Action-Oriented Landing Page in the Industrial Workspace so that your users can access their critical tasks.

The following table lists the Guided Setup tasks and their purposes for the OT Action-Oriented Landing Page.

OT Action-Oriented Landing Page setup tasks

Task	Purpose
1. Set the system properties for the OT Action-Oriented Landing Page.	Changes the amount of cards shown under **Important Actions** with the sn_mfg_common.landing_page_important_actions_limit system property.

Set the system properties for the Operational Technology Action-Oriented Landing Page

Set the system properties for the Operational Technology (OT) Action-Oriented Landing Page so that you can enable the properties as needed.

Before you begin

Role required: configure_industrial_workspace

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Workspace System Properties**.
2. Edit the following properties as needed.

System property	Description
OT Home (Action-Oriented Landing Page) system properties	
sn_mfg_common.landing_page_important_actions_limit	Maximum number of Important Actions fetched for the **Important Actions** section in the OT Action-Oriented Landing Page. The default is 50.

3. Select **Save**.

Setting up the Operational Technology Progress Scorecard

Set up the Operational Technology (OT) Progress Scorecard in the Industrial Workspace so that your users can compare site data and progress.

The following table lists the Guided Setup tasks and their purposes for the OT Progress Scorecard.

OT Progress Scorecard setup tasks

Task	Purpose
1. Assign the OT Progress Scorecard roles.	Assign the OT Progress Scorecard roles to your users so that you can control their access to the features, capabilities, and data for OT Progress Scorecard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Progress Scorecard setup tasks (continued)

Task	Purpose
2. Validate the completeness score calculation.	Validate that the **CMDB Health Dashboard - Completeness Score Calculation** is activated to run if you want to include the **OT Device Data Completeness (%)** indicator in the OT Progress Scorecard.
3. [Optional] Review the indicator sources.	Reviews the indicator sources for a larger number of records. If you expect more than the default value of 1 million total records, you must override the records collection.
4. Configure the expected OT devices for a site.	Configure the number of expected OT devices for a site so that you can use the **% of Expected OT Devices in CMDB** indicator in the OT progress scorecard.
5. Complete the [PA OTPSC] Monthly Data Collection job.	Collects and displays the daily data for all indicators from Performance Analytics for the OT Progress Scorecard tab. You must complete this step before others can view the data in this tab.
6. Configure the OT Progress Scorecard indicators.	Configure the OT Progress Scorecard indicators so that the display of each indicator meets your needs.
7. Set the system properties for the OT Progress Scorecard.	Configures the thresholds shown on the OT Progress Scorecard and the components used to determine the calculated score.
8. Customize the module name.	Customize the module name of the OT Progress Scorecard to change its name from the default value with a name more suitable for your needs.

Assign the Operational Technology Progress Scorecard roles

Assign the Operational Technology (OT) Progress Scorecard roles to your users so that you can control their access to the features, capabilities, and data for OT Progress Scorecard.

Before you begin

Role required: admin

About this task

Users with the role that are listed in the following table can use the OT Progress Scorecard.

OT Progress Scorecard role

Role	Description
OT Progress Scorecard Viewer [ot_progress_scorecard_viewer]	Can view the OT Progress Scorecard with all site data available.
OT Progress Scorecard Editor [ot_progress_scorecard_editor]	Can view and edit the OT Progress Scorecard with all site data available.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Validate the completeness score calculation

Validate that the **CMDB Health Dashboard - Completeness Score Calculation** is activated to run if you want to include the **OT Device Data Completeness (%)** indicator in the Operational Technology (OT) Progress Scorecard.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup**.
2. In the **Industrial Workspace** section, select **OT Progress Scorecard**.
3. In the **Validate Completeness Score Calculation** task, select **Configure**.
4. In the **CMDB Health Dashboard - Completeness Score Calculation** Scheduled Script Execution record, validate the following items:
   a. Validate that the **Active** check box is checked.
   b. To ensure accurate scores are collected for end of the month reporting, validate that **Run** field is configured
5. Select **Update**.

For more details on how completeness is calculated, see the **Completeness** section of CMDB Health KPIs and metrics.

Review the indicator sources for a large number of records

Review the indicator sources if you need a large number of records. You can override the records collection so that the Operational Technology (OT) Progress Scorecard shows more records than the default value of 1 million.

Before you begin
Role required: admin or pa_admin

About this task
Due to the migration with Performance Analytics, each indicator of the OT Progress Scorecard can only show 1 million records by default. If you have the admin or pa_admin role and the records exceed 1 million after running the [PA OTPSC] Monthly Data Collection, an error message directs you to the job logs.

Note: If you don't have the admin or pa_admin role and the records exceed 1 million after running the [PA OTPSC] Monthly Data Collection job, an error message directs you to contact an administrator for help.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you have the admin or pa_admin role, you can check the job logs related list from the link in the error message and filter out the information to see which indicator source has the error. After you find the indicator source with the error, you can change the indicator sources for a larger number of records and override the indicator source data. Then, an error message no longer appears for the other users and the data is shown for the indicator source. For more information about the indicator sources, see Indicator sources.

Note: If you need to create new indicators, you must use the site breakdown included in the Industrial Workspace Common. The site breakdown part of the Operational Technology Manager application is deprecated.

The job logs may include errors that aren't about the indicator sources. You must filter the job logs record by the **Level** column and find the error messages about the indicator sources.

Procedure

1. Navigate to **All** > **Performance Analytics** > **Sources** > **Indicator Sources**.
2. Apply a filter by selecting the Show/hide filter ( ) icon and add the following filter:
   `[Application] [is] [Industrial Workspace Common]`
3. Select the indicator source record that you need to change.
   You can find which indicator source needs to be adjusted from the job logs link in the error message.
4. On the **Records Collection** tab, select the check box next to the **Override records collection** field.
5. In the **Maximum number of fetched records** field, change the value to `XM`.
6. Select **Update**.

Configure the expected OT devices for a site

Configure the number of expected OT devices for a site so that you can use the **% of Expected OT Devices in CMDB** indicator in the OT progress scorecard.

Before you begin

Role required: ot_progress_scorecard_editor and cmdb_ot_isa_viewer with site access assigned for relevant sites through user criteria

Note: For more information about site access through user criteria, see Review the homepage destination rules for the Industrial Workspace.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **OT Progress Scorecard Attributes**.
2. If you need to create a record with your site, complete these actions.
   a. Select **New**.
   b. In the **Site** field, add your site.
   c. In the **Value** field, add the number of expected OT devices for that site.

      Note: Don't include OT control modules in this value.

   d. Select **Save**.
3. If a record with your site exists and you want to modify the expected devices, complete these actions.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the record you want to edit.

b. In the **Value** field, modify the number of expected OT devices for that site.

> **Note:** Don't include OT control modules in this value.

c. Select **Update**.

Configure the data collection for the Operational Technology Progress Scorecard

Configure the data collection for Operational Technology (OT) Progress Scorecard so that you can collect and display the daily data for all indicators from Performance Analytics. This configuration ensures that your OT data is displayed accurately on the scorecard.

Before you begin

Role required: admin or pa_admin

About this task

If you don't run the [PA OTPSC] Monthly Data Collection job, then no data is available for the OT Progress Scorecard. If you have the admin role, you see a warning message that prompts you to run the job.

> **Note:** If you don't have an admin role, you see a warning message that prompts you to reach out to the administrator for help.

Procedure

1. Navigate to **All** > **Data Collector** > **Performance Analytics** > **Jobs**.
   If you're in the OT Progress Scorecard, navigate to the Scheduled Data Collection table by selecting **Run job now** in the error message.
2. Apply a filter by selecting the Show/hide filter ( ) icon and add a filter of `[Name] [is] [[PA OTPSC] Monthly Data Collection]`.
3. Start collecting the data by selecting the check box next to the **Active** field in the Job parameters section and then schedule a time in the **Time** field.
   You can collect the data manually, by using the **Execute Now** button. Otherwise, no data is shown when you view the tab. Only use the **Execute Now** button when you first run the job. The data that is collected after this point should be collected at a scheduled time.
4. Check if the default schedule collection time works for you.
   The default time is 00:00:00 at the beginning of every month. If you want to change the default collection time, you can change it after activating the job. Make sure that you notify your users about this change.

Result

The OT Progress Scorecard is now showing the correct site data for your users.

> **Note:** The OT Progress Scorecard uses Performance Analytics. Performance Analytics only saves the scores for 5 months. If want to preserve your scores and compare site data for more than 5 months, see Activating your Performance Analytics subscription.

Configure an indicator by threshold, weightage, and order

Configure the Operational Technology (OT) Progress Scorecard indicators so that the display of each indicator meets your needs.

Before you begin

Role required: ot_progress_scorecard_editor or configure_industrial_workspace

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

You can configure the following indicators.

- Overall Score (%)
- % of Expected OT Devices in CMDB
- Classified OT Devices (%)
- Assigned OT Devices (%)
- OT Device Data Completeness (%)
- Mapped OT Devices (%)
- Backed up OT Devices (%)
- Approved OT Change Requests (%)
- OT Incidents with OT Context (%)

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **OT Progress Scorecard Config**.
2. Select the indicator you want to edit.
3. On the form, fill in the following fields.

Indicator configuration fields

Field	Description
Low Threshold	The lowest threshold that the indicator can meet.
High threshold	The highest threshold that the indicator can meet.
Weightage	The total weightage that the indicator contributes to the overall score.
Order	The rank of the indicator by importance from left to right.

4. If you do not need an indicator to be shown, set de-select the **Active** field.
5. Select **Update**.

Set the system properties for the Operational Technology Progress Scorecard

Set the system properties for the Operational Technology (OT) Progress Scorecard so that you can enable the properties as needed.

Before you begin

Role required: configure_industrial_workspace

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Workspace System Properties**.
2. Edit the following properties as needed.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

System property	Description
OT Progress Scorecard configuration	
sn_mfg_common.otpsc.page_title	The page title shown on the OT Progress Scorecard. The default is `OT Progress Scorecard`.
sn_mfg_common.otpsc.records_per_page	The number of records shown per page. The default is `10`.
sn_mfg_common.otpsc.low_threshold_color	A color to represent the low threshold in the OT Progress Scorecard.
sn_mfg_common.otpsc.medium_threshold_color	A color to represent the medium threshold in the OT Progress Scorecard.
sn_mfg_common.otpsc.high_threshold_color	A color to represent the high threshold in the OT Progress Scorecard.

3. Select **Save**.

Customize the module name

Customize the module name of the Operational Technology (OT) Progress Scorecard to change its name from the default value with a name more suitable for your needs.

Before you begin

Role required: admin or ui_builder_admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup**.
2. In the **Industrial Workspace** module, select the **OT Progress Scorecard section**.
3. In the **[OPTIONAL] Customize Module Name** task, select **Configure**.
4. In the **Value** field, edit the `"message"` value from `OT Progress Scorecard` to a name that fits your needs.
5. Select **Update**.

Setting up the Operational Technology Visibility dashboard

Complete the Guided Setup tasks so that you can start setting up the Operational Technology (OT) Visibility dashboard with the data collections, indicator resources, and filters for your organization.

To access the Guided Setup for the OT Visibility dashboard, navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** and select the Operational Technology Visibility Dashboard section under Operational Technology Manager.

For more information about the OT Visibility dashboard and its contents, see Operational Technology Visibility dashboard.

The following table shows the Guided Setup tasks used to set up the dashboard.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Visibility dashboard Guided Setup tasks

Task	Purpose
1. Complete the OT Devices Daily Data Collection job.	Collects and displays the daily data for all indicators from Performance Analytics for the OT Visibility dashboard. You must complete this step before others can view the dashboard data.
2. [Optional] Review the indicator sources.	Reviews the indicator sources for a larger number of records. If you expect more than the default value of 1 million total records, you must override the records collection.

Configure the data collection for Operational Technology devices

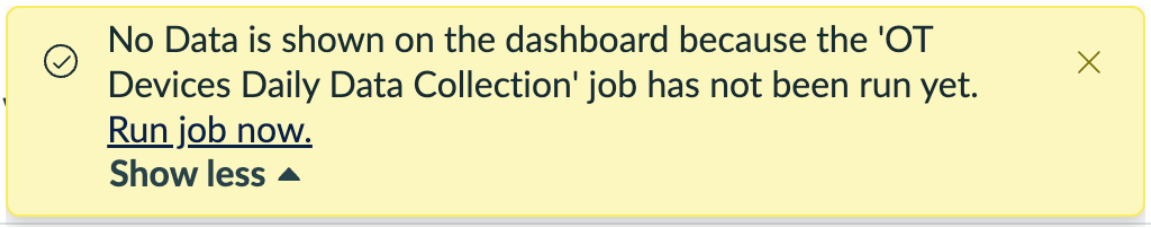
Configure the data collection for Operational Technology (OT) devices so that you can collect and display the daily data for all indicators from Performance Analytics. This configuration ensures that your OT data is displayed accurately on the OT Visibility dashboard.

Before you begin

Role required: admin or pa_admin

About this task

If the OT Devices Daily Data Collection job hasn't run yet, that means that no data is available for the OT Visibility dashboard and the **Last updated** timestamp is hidden. If you have the admin role, you see the following warning message that prompts you to run the OT Devices Daily Data Collection job:



Note: If you don't have the pa_admin role, you see a warning message that prompts you to reach out to the administrator for help.

Procedure

1. Navigate to **All** > **Data Collector** > **Performance Analytics** > **Jobs**.
   If you're in the OT Visibility dashboard, you can navigate to the Scheduled Data Collection table by selecting **Run job now** in the error message.
2. Apply a filter by selecting the Show/hide filter ( ) icon and add a filter of `[Name] [is] [OT Devices Daily Data Collection]`.
3. Start collecting the data by selecting the check box next to the **Active** field in the Job parameters section and then schedule a time in the **Time** field.
   You can collect the data manually by using the **Execute Now** button. Otherwise, no data is shown when you view the dashboard. Only use the **Execute Now** button when you first run the job. The data that is collected after this point should be collected at a scheduled time.
4. Check if the default schedule collection time works for you.
   The default time is 00:00:00 daily. If you want to change the default collection time, you can change it after activating the job. Make sure that you notify your users about this change.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
The OT Visibility dashboard is now showing the correct data for the collected OT devices for your users.

What to do next
Now, you can review the indicator sources and determine if you need to override the default records collection. For more information, see Review the indicator sources for a large number of records.

Review the indicator sources for a large number of records

Review the indicator sources if you need a large number of records. You can override the records collection so that the Operational Technology (OT) Visibility dashboard shows more records than the default value of 1 million.

Before you begin
Role required: admin or pa_admin

About this task
Due to the migration with Performance Analytics, each indicator of the OT Visibility dashboard can only show 1 million records by default. If you have the admin or pa_admin role and the records exceed 1 million after running the OT Devices Daily Data Collection job, an error message directs you to the job logs.

Note: If you don't have the admin or pa_admin role and the records exceed 1 million after running the OT Devices Daily Data Collection job, an error message directs you to contact an administrator for help.

If you have the admin or pa_admin role, you can check the job logs related list from a link in the error message and filter out the information to see which indicator source has the error. After you find the indicator source with the error, you can change the indicator sources for a larger number of records and override the indicator source data. Then, an error message no longer appears for the other users and the data is shown for the indicator source. For more information about the indicator sources, see Indicator sources.

Note: If you need to create new indicators, you must use the site breakdown included in the Industrial Workspace Common. The site breakdown part of the Operational Technology Manager application is deprecated.

The job logs may include errors that aren't about the indicator sources. You must filter the job logs record by the **Level** column to find the error messages about the indicator sources.

Procedure
1. Navigate to **All** > **Performance Analytics** > **Sources** > **Indicator Sources**.
2. Apply a filter by selecting the Show/hide filter ( ) icon and add the following filters.
   - `[Application] [is] [Operational Technology Manager]`
   - `[Facts table] [is] [cmdb_ci]`

   After applying the filters, the table shows the following device indicator records:
   - Benchmark: Inactive OT Devices
   - Benchmark: Industrial IoT
   - Benchmark: New OT Devices Discovered
   - Benchmark: OT Computer and Servers
   - Benchmark: OT Devices

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Benchmark: OT Network Gear
- Benchmark: Unmapped OT Devices

3. Select the indicator source record that you need to change.
   You can find which indicator source needs to be adjusted from the job logs link in the error message.
4. On the **Records Collection** tab, select the check box next to the **Override records collection** field.
5. In the **Maximum number of fetched records** field, change the value to `XM`.
6. Select **Update**.

Setting up the Operational Technology Vulnerability Response (PA) dashboard

Set up the Operational Technology Vulnerability Response (PA) dashboard in the Industrial Workspace so that your users can access their critical tasks.

The following table lists the Guided Setup tasks and their purposes for the Operational Technology Vulnerability Response (PA) dashboard.

Operational Technology Vulnerability Response (PA) dashboard setup tasks

Task	Purpose
1. Configure the data collection jobs.	Collects and displays the daily data for all indicators from Performance Analytics for the OTVR (PA) dashboard. You must complete this step before others can view the data in this tab.
2. [Optional] Review the indicator sources.	Reviews the indicator sources for a larger number of records. If you expect more than the default value of 1 million total records, you must override the records collection.

Configure the data collection for the Operational Technology Vulnerability Response (PA) dashboard

Configure the data collection for the data shown on the Operational Technology Vulnerability Response (PA) dashboard. Scheduled jobs are automated pieces of work that can be performed at a specific time or on a recurring schedule.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Data Collector** > **Performance Analytics** > **Jobs**.
2. Apply a filter by selecting the Show/hide filter ( ) icon and add the following filters .
   - `[Application] [is] [Operational Technology Vulnerability Response]`
   - `[Class] [is] [Scheduled Data Collection]`

   The following scheduled jobs appear when you apply the filter.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- [PA OT VR] Historical Vulnerability Data Collection

  Note: The [PA OT VR] Historical Vulnerability Data Collection job is an on-demand job that you only need to execute once. After the historical data is collected, the daily data collection jobs run on a scheduled time every day. For more information about historical data, see Collect historical data.

- [PA OT VR] Daily Collection for Remediation Tasks
- [PA OT VR] Daily Collection for Vulnerable Items 1
- [PA OT VR] Daily Collection for Vulnerable Items 2
- [PA OT VR] Daily Collection for Vulnerable Configuration Items (CIs)

3. To start collecting the data, select a scheduled job record.
4. Select the check box next to the **Active** field in the Job parameters section and then schedule a time in the **Time** field.
   You can collect the data manually, by using the **Execute Now** button. Otherwise, no data is shown when you view the tab. Only use the **Execute Now** button when you first run the job. The data that is collected after this point should be collected at a scheduled time.
5. Check if the default schedule collection time works for you.
   The default time is 00:00:00 daily. If you want to change the default collection time, you can change it after activating the job. Make sure that you notify your users about this change.
6. Repeat steps 3 to 5 for each scheduled job.

Result

The Operational Technology Vulnerability Response (PA) dashboard is now showing the correct data for your users.

What to do next

Now, you can review the indicator sources and determine if you need to override the default records collection. For more information, see Review the indicator sources for a larger number of records.

Review the indicator sources for a larger number of records

Review and update an indicator source to override the expected record count if you expect more than 1 million records to be collected from the indicator sources. This action helps to avoid system performance issues when collecting data for the Industrial Workspace.

Before you begin

Role required: admin or pa_admin

Procedure

1. Navigate to **All** > **Performance Analytics** > **Indicators** > **Automated Indicators**.
2. Apply the filter **[Application] [is] [Operational Technology Vulnerability Response]**.
3. Under the Indicator Source column, select the indicator source record that you want to edit.
4. In the Records collection section, select the check box next to the **Override record collection** field.
5. In the **Maximum number of fetched records** field, add a number greater than the default value of 1 million records.
   For example, **2 million**.
6. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setting up the Operational Technology Unified Map experience

Set up the Operational Technology (OT) Unified Map experience in the Industrial Workspace so that your users can access Unified Maps.

The following table lists the Guided Setup tasks and their purposes for the OT Unified Map experience. The admin role is required.

Note: These Guided Setup tasks are optional to complete as they modify the default settings of the available configuration identifier.

These configuration identifier settings affect all users. Individual users cannot configure the settings.

OT Unified Map experience setup tasks

Task	Purpose
Modify the default settings of the Industrial Workspace Config Identifier.	Modify the following default settings of the Industrial Workspace Config Identifier to configure the OT Unified Map experience: • Workspace configuration properties • Node map profiles • Node map related items • Operational life cycle modes • Table attributes

Default settings of the Operational Technology Unified Map experience

You can modify the default settings available for the Operational Technology (OT) Unified Map experience.

With the **admin** or **sn_cmdb_ws.config_admin** role, you can modify the default settings of the Industrial Workspace Config Identifier available with the OT Unified Map experience. A configuration identifier, or config identifier, is a configuration element within the configuration identifiers framework. A config identifier contains settings and table-driven configurations used in a UX application such as a workspace.

If a property isn't set or if there are no entries in the table-driven configuration, look-up uses the values in the default configuration identifier instead. For more information about the configuration identifiers framework, see Configuration identifiers framework.

To access the Industrial Workspace Config Identifier record, navigate to **All**, and in the filter bar, enter `sn_cmdb_ws_config_identifier.list`. Then select **Industrial Workspace Config Identifier**.

The following sections describe the default settings available to modify in the Industrial Workspace Config Identifier.

Note: The settings described affect all users. Individual users can’t configure the settings.

Workspace Config Properties

By default, the following configuration properties are listed in the `sn_cmdb_ws_config_property.list` and are assigned to the default configuration identifier.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- unifiedmap.map_search.max_nodes
- unifiedmap.map_search_filter.default_levels
- unifiedmap.map_search_filter.max_levels
- unifiedmap.map_search_filter.endpoint_deduplication_fields

Node Map Profiles

You can configure profiles that set default map filters and default map orientation for a class. For example, to show the service-mapping data for the Mapped Application Service class.

These class profiles help in identifying which layers are shown on the Unified Map for a given configuration item (CI) node. Class profiles are applied when no filter preset is used with the current map. This application typically occurs when you initially load a map without a filter preset, or when you set the filter preset to the default view.

With class profiles, you can only configure the **Layer** category in the filter panel.

Node Map References

Map references enable connections on the map between CIs from two classes that aren't connected by a relationship.

Node Map Related Items

You can use the Related Items module in the Unified Map to set the related items categories that appear for CIs, such as active incidents and active problems. When you select the Related Items module, related items are grouped by categories in the contextual side panel.

Operational life cycle modes

You can specify the operational states that CIs must have for them to be included in the Unified Maps.

Table Attributes

Each class has a unique set of extended properties that appear in the Unified Map Attributes panel for a CI. Many common classes are preconfigured with these properties. You can modify the default settings and globally configure extended properties for additional classes.

Set up the Hardware Vulnerability Assessment of Operational Technology devices using guided setup

Use the Industrial Workspace Admin guided setup to walk you through configuring the Hardware Vulnerability Assessment feature available on the Industrial Workspace menu.

Before you begin

Role required: admin

About this task

Use the Industrial Workspace Admin guided setup to assign required user roles, configure a system property, and schedule jobs to perform the hardware vulnerability assessment of Operational Technology devices.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > *Operational Technology Vulnerability Response*.
2. Select **Get Started** for the *Operational Technology Vulnerability Response* application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select the *Hardware Vulnerability Assessment* task.
4. Select the following task tabs, then select **Configure** to complete the configuration tasks.

Task	Purpose
User Roles assignment	Assign users or user groups with roles that en able them to use the Hardware Vulnerability Assessment feature.
Install and Run NVD Integration	Run the National Vulnerability Database (NVD) integration to import data from the NIST NVD database to help you determine the severity and details of CVEs found in your en vironment.
Configure Vulnerability Assessment proper ties	Configure the properties required to perform hardware vulnerability assessment for OT de vices.
Schedule Vulnerability Assessment Jobs	Execute scheduled jobs that enable vulnera bility assessment on OT devices in the inven tory and mark expired assessments that must be deleted.
Normalization opt-in	Select **Firmware Discovery Model** Opt-in op tion for ServiceNow Asset Management Con tent Service to collect unnormalized firmware details of OT devices and update the normal ized content library. This process improves the ratio of normalized data mapping to CVEs and therefore improves assessment of vulner abilities.
Delete obsolete assessments	Configure the time duration after which the obsolete and expired assessments are delet ed.

Related topics

Guided Setup

Operational Technology Hardware Vulnerability Assessment

Assign roles for Hardware Vulnerability Assessment

Assign roles to users so that they can configure properties, and use hardware vulnerability assessments features, capabilities, and data.

Before you begin

Role required: admin or user_admin

About this task

Assign the following roles to users and user groups or Hardware Vulnerability Analyst users#br user groups that are listed in the following table:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Hardware Vulnerability Assessment Roles

Role	Description
[sn_vul.manage_exposure_assessment]	Can view or edit properties for Hardware Vulnerability Assessment.
OT Vulnerability Event Manager [sn_otvr.vul_event_manager]	Can view and perform assessments related to Hardware Vulnerability Assessment.

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Hardware Vulnerability Assessment** > **Configure User Roles assignment** > **Configure**.
   Alternatively, you can navigate to **User Roles assignment** > **Configure** > **Users**.
2. Assign roles to users and groups by using the ServiceNow AI Platform user administration feature.

Task	User administration feature
Assign a role to a user	See
Assign a role to a group	See

Run NVD Integrations for Hardware Vulnerability Assessment

Install and run National Vulnerability Database (NVD) integrations to perform hardware vulnerability assessment.

Before you begin

Role required: sn_otvr.vul_event_manager and admin

About this task

Hardware Vulnerability Assessment is based on the vulnerability assessment feature in Vulnerability Response. You must HVA run the NVD integrations to access the Common Vulnerabilities and Exposures (CVEs) data in the NVD database.

To understand what are the different NVD integrations and how do the integrations work, see:

- National Vulnerability Database (NVD) integration
- Install the Vulnerability Response Integration with the NIST National Vulnerability Database

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Hardware Vulnerability Assessment** > **Configure Install and Run NVD Integration** > **Configure**.
   Alternatively, you can navigate to **All** > **Vulnerability Response** > **Administration** > **Integrations**
2. Install and execute the following NVD Integrations:

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- *NIST National Vulnerability Database Integration-API (CVE only)*
- *NIST National Vulnerability Database Integration-API (CPE only)*
- *NIST National Vulnerability Database Integration-API (Unmapped CPE)*

Configure properties for Hardware Vulnerability Assessment

Configure the properties required to perform hardware vulnerability assessment.

Before you begin

Role required: sn_vul.manage_exposure_assessment and admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Hardware Vulnerability Assessment** > **Configure Vulnerability Assessment Properties** > **Configure** > **Vulnerability Assessment**.
   Alternatively, you can navigate to **All** > **Vulnerability Response** > **Administration** > **Properties** > **Vulnerability Assessment**.
2. Perform the following configurations.

Property	Description
`sn_vul_analyst.auto_create_vits`: **This property determines if new vulnerable item records will be created automatically for fully matched hardware vulnerability assessments. When set to true, new vulnerable item records are created automatically for fully matched hardware vulnerability assessments.**	Select **Yes**. The default value is **Yes**. When set to **Yes**, new vulnerable item records are created automatically for fully matched hardware vulnerability assessments. Deselect if you want to create vulnerable items (VITs) manually.
`sn_vul_analyst.assess_unmapped_disc_models`: **Enabling this property includes discovery models without CPE mappings in the assessment.**	The default value is **No**. Select **Yes** to perform vulnerability assessments for discovery models of OT devices that aren't CPE-mapped.
`hva_confidence_score_threshold`: **This property controls the minimum confidence score threshold required for creation of vulnerability assessments. Only matches with scores equal to or above this threshold will generate vulnerability assessments. The threshold value must be a decimal number between 0.0 and 1.0. Default value OOB is 0.75.**	Edit the value according to your requirement. The default value is 0.75. **Note:** You can set the value for Confidence Score to 0. But an assessment won't be created with 0 Confidence Score.

3. Select **Save**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Run scheduled jobs to perform Hardware Vulnerability Assessment

Execute scheduled jobs to perform hardware vulnerability assessment.

Before you begin

Role required: sn_otvr.vul_event_manager and admin

About this task

You must perform the following scheduled jobs to detect firmware vulnerabilities of any OT devices in the inventory:

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Hardware Vulnerability Assessment** > **Scheduled Vulnerability Assessment Jobs** > **Configure** > **Scheduled Jobs**.

   Important:

   - You must run *Hardware Assessment - Full* before you schedule the *Hardware Assessment - Delta* job. You can run the *Hardware Assessment - Full* on demand.
   - You can schedule *Hardware Assessment - Delta* job to run daily, weekly, or according to your required frequency.

2. Select **Hardware Assessment - Full** > **Execute Now**.
   This job performs an assessment on all OT devices in the inventory to detect any firmware vulnerabilities regardless of prior assessments.
3. Select **Hardware Assessment - Delta** > **Active**.

   Select **Run** and choose a frequency from the list. The **Hardware Assessment - Delta** job runs according to the frequency that you select.

   This job performs incremental assessments, targeting only changes or updates since the last assessment run. It captures changes on firmware, normalized contents, and vulnerabilities since the last successful run of the hardware vulnerability assessment. This job makes sure that you can maintain continuous monitoring and timely updates.
4. Select **Hardware Vulnerability Assessment - Mark Expired Assessments** > **Active** to start this job.

   Select **Run** and choose a frequency from the list. The *Hardware Vulnerability Assessment - Mark Expired Assessments* job runs according to the frequency that you select.

   Hardware vulnerability assessments are based on the firmware data available for a device. If you update the firmware version of a device, the existing assessments based on the previous firmware version are no longer valid and are considered as expired assessments. You can delete expired assessments, which are older than a month. However, you must perform new vulnerability assessments for the devices with an updated firmware version.

Related topics

Scheduled jobs

Configure Normalization Opt-in for Hardware Vulnerability Assessment

Select **Firmware Discovery Model** Opt-in option for ServiceNow Asset Management Content Service to collect unnormalized firmware details of Operational Technology (OT) devices and

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

update the normalized content library. This process improves the ratio of normalized data mapping to CVEs and therefore improves assessment of vulnerabilities.

Before you begin
Role required: sn_eam.enterprise_admin or admin

Procedure

1. Navigate to **All** > **Industrial Workspace Admin** > **Guided Setup** > **Operational Technology Vulnerability Response** > **Hardware Vulnerability Assessment** > **Normalization opt-in** > **Configure**.
2. Select **Yes**.
3. Enable **Firmware Discovery Models** toggle button.

Related topics

Opt-in to the Enterprise Asset Management Content Service

Delete obsolete and expired hardware vulnerability assessments

Set up automatic deletion of obsolete or expired assessment records.

Before you begin
Role required: admin

About this task
Configure the age of obsolete or expired assessments to be cleaned.

- Obsolete assessments: Invalid assessments, which have been ignored or the associated vulnerable items (VITs) are closed for more than two years.
- Expired assessments: If you update the firmware version of a device, the existing assessments based on the previous firmware version become invalid and are considered as expired assessments. You can delete expired assessments, which are older than a month. However, you must perform new vulnerability assessments for the devices with an updated firmware version.

Procedure

1. Navigate to **All** > **System Data Management** > **Data Management Policies**.
2. Search for and select the **sn_vul_analyst_firmware_vulnerability_assessment** policy.
3. Select the **Active** check box and configure clean-up rules according to your requirement. Configure the age in clean-up rules 1, 2, and 3, after which the obsolete and expired assessments are deleted:
   - Rule 1: Delete firmware vulnerabilities assessment whose VIT is closed since 2 years(based on last update date on VIT associated).
   - Rule 2: Delete firmware vulnerabilities assessment which are ignored since 2 years (based on created date).
   - Rule 3: Delete firmware vulnerabilities assessment which are expired since 1 month (based on last update date).
4. Select **Update**.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Setting up the OT Network Map

Set up the Operational Technology (OT) Network Map so that you can access the map in the in the Industrial Workspace.

The following table lists the setup tasks for the OT Network Map. The admin role is required.

OT Network Map setup tasks

Task	Purpose
Run the OT Network Map Cache Handler scheduled job	Configure this scheduled job to run after your Service Graph Connectors to populate the latest data to show in Node Map.
Set the system property for the OT Network Map	Set the **Max CI Nodes per Site (sn_ot_core.node_map.max_ci_nodes_per_site)** system property to determine the maximum number of CI nodes shown per site on the network map.

Run the OT Network Map Cache Handler scheduled job

Configure this scheduled job to run after your Service Graph Connectors to populate the latest data to show in the OT Network Map.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
2. Select the **OT Network Map Cache Handler** scheduled job.
3. Select **Execute Now**.

Result
The scheduled job runs after the Service Graph Connectors, and the data used to create the nodes in the OT Network Map is populated.

Set the system property for the OT Network Map

Set the **Max CI Nodes per Site (sn_ot_core.node_map.max_ci_nodes_per_site)** system property to determine the maximum number of configuration item (CI) nodes shown per site on the OT Network Map.

Before you begin
Role required: admin

Procedure

1. Navigate to **All** > **System Properties** > **All**.
2. Select the **sn_ot_core.node_map.max_ci_nodes_per_site** system property record.
   To find this system property, you can set a filter by selecting the **Show / hide filter** Filter icon and applying a **[Name] [is] [sn_ot_core.node_map.max_ci_nodes_per_site]** filter value.
3. If needed, edit the **Value** field to change the number of CI nodes shown per site.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Note: The default value is 10K. If a site has more than 10K CIs, then the additional CIs aren't considered in the network map calculations.

4. Select **Update**.

Using the Industrial Workspace

After you complete all the required set-up tasks for the Industrial Workspace, users can begin managing their Operational Technology data on the different pages and dashboards available in the Industrial Workspace.

Industrial Workspace homepage destination rules

Depending on your assigned roles, you're redirected to different pages in the Industrial Workspace with homepage destination rules. This helps you access the data that you need more quickly and efficiently.

Homepage destination rules overview

Each destination rule redirects different OT users to different pages on the Industrial Workspace based on their assigned role or roles. Some roles may not have access to the data on one page, so redirecting users to a page where data is available to view helps them better navigate the Industrial Workspace. For example, users with only the Operational Technology Editor [cmdb_ot_editor] role can't view data on the OT Action-Oriented Landing Page, so they only see the an empty landing page. Instead, they're redirected to the Industrial Workspace Lists, where they can view the applicable OT device data.

Industrial Workspace homepage destination rule descriptions

The following table describes the Industrial Workspace homepage destination rules and their destinations.

Homepage destination rules

Rule	Destination	Roles redirected	Description
OT Progress Scorecard Page	now/mfg/ot-progress-scorecard/ (OT Progress Scorecard)	ot_progress_scorecard_viewer	The OT Progress Scorecard rule takes users with the roles described in the rule directly to the OT Progress Scorecard when they log in.
Industrial Workspace Home Page	now/mfg/home (OT Action-Oriented Landing Page)	• sn_ot_incident_read • sn_ot_change_read • sn_otvr.remediation_owner	The Industrial Workspace Home Page rule takes users with the roles described in the rule directly to the OT Action-Oriented Landing Page when they log in.
OT Dashboard Library Page	now/mfg/dashboard-library (OT Dashboard Library)	cmdb_ot_viewer + cmdb_ot_isa_viewer	The OT Dashboard Library Page rule takes users with the

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Homepage destination rules (continued)

Rule	Destination	Roles redirected	Description
			roles described in the rule directly to the OT Visibility dashboard when they log in. **Note:** The OT Dashboard Library Page rule only displays if Operational Technology Manager is installed.
ISA Equipment Model Page	now/mfg/isa-equipment-model (Equipment Model Manager)	cmdb_ot_isa_viewer	The ISA Equipment Model Page rule takes users with the roles described in the rule directly to the Equipment Model Manager when they log in. **Note:** The ISA Equipment Model Page rule only displays if Industrial Process Manager is installed.
Industrial Workspace List Page	now/mfg/list (Industrial Workspace Lists)	cmdb_ot_viewer	The Industrial Workspace List Page rule takes users with the roles described in the rule directly to the Industrial Workspace Lists when they log in.

Search for a record in the Industrial Workspace

Search for a record in the Industrial Workspace related to Operational Technology (OT) data, or Configuration Management Database (CMDB) data.

Before you begin

- This search experience applies only to instances with AI Search as its search engine. Instances with Zing as its search engine have a different search experience.
- Role required: cmdb_ot_viewer

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

About this task

The Industrial Workspace search is configured to show Natural Language Query (NLQ) Genius Results for each search. For more information about how NLQ Genius Results are used in the Industrial Workspace, see NLQ Genius Results used in the Industrial Workspace. For more information about NLQ Genius Results, see NLQ Genius Results.

Using the search bar in the Industrial Workspace, you can search and find results for the following records.

- IT Incident
- OT Incident and Incident Task

  Note: OT Incident and Incident Task records are only available if you have Operational Technology Incident Management installed.

- OT Change and Change Task

  Note: OT Change and Change Task records are only available if you have Operational Technology Change Management installed.

- Catalog Task
- Knowledge
- User

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. In the Search bar, use key words or the record number to search for a record.
3. In the search results, select the record you want to view.
   If you select a tab and don't have access to the returned records, you will see a **No Results** message.
4. If you're not in the Industrial Workspace but want to search for records in the Industrial Workspace, perform the following actions.
   a. In the Search bar, select the **Choose search context** ( ) icon.
   b. From the drop-down, select **Industrial Workspace**.

NLQ Genius Results used in the Industrial Workspace

The Industrial Workspace leverages Natural Language Query (NLQ) Genius Results for each search.

NLQ Genius Results overview

Configuration Management Database (CMDB) tables cannot be indexed by AI Search. The Industrial Workspace search is configured to show NLQ Genius Results for each search, which can be used to search CMDB tables. NLQ Genius Results use NLQ processing to surface relevant results from tables that match your search query.

For more information about NLQ Genius Results, see NLQ Genius Results.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Searching OT CIs

You can search Operational Technology (OT) configuration items (CIs) by specifying the table and column, leveraging the NLQ Genius Results.

The following table contains examples for searching different information for a PLC. If there are additional columns you need to search, you can follow this general pattern.

Information type	Search input
Searching for a PLC by name	`PLC Name <insert name>`
Searching for a PLC by model ID	`PLC Model ID <insert model ID>`
Searching for a PLC by description	`PLC Description <insert description>`
Searching for a PLC by manufacturer	`PLC Manufacturer <insert manufacturer>`

Site filter in the Industrial Workspace

You can use the site filter in the Operational Technology (OT) Visibility dashboard, the Operational Technology Vulnerability Response (PA) dashboard, and the OT Vulnerability Risk Rollup dashboard to view data for specific sites.

The site filter lets you specify the OT device or vulnerability data that you want to see on the following dashboards.

- OT Visibility dashboard
- OTVR (PA) dashboard
- OT Vulnerability Risk Rollup dashboard

To use the site filter, you must have the **cmdb_ot_isa_viewer** role with access to the site you want to view.

The site filter lets you do the following actions:

- Search for a specific site.
- View the OT data for one or multiple sites.
- View the OT data for no site assigned.

> **Note:** If there's no site assigned to an OT device, the filter shows **No site assigned**. To have the correct sites shown on the dashboard, you must assign a site to the device and then assign a business unit to that site.

Use the site filter

Filter dashboard data by site in the Operational Technology (OT) Visibility, Operational Technology Vulnerability Response (PA), and the Operational Technology (OT) Risk Rollup dashboards.

Before you begin
Role required: cmdb_ot_isa_viewer with site access

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the **Dashboard Library** () icon.
3. Select either the OT Visibility dashboard or the Operational Technology Vulnerability Response dashboard.
4. Select **Site** to display the list of available sites.
5. Select any site to view the dashboard data.
6. To apply one or more sites to the dashboard, complete the following actions.
   a. In the **Available** column, select each site that you want to view data for.
   b. To move your selected site or sites to the **Applied** column, click the **Move selected items** icon  .

Operational Technology Progress Scorecard filters

You can use the filters on the Operational Technology (OT) Progress Scorecard to specify the data that you want to see on your scorecard by site, business unit (BU), or date.

Scorecard filter overview

The business unit, site, and date filters let you specify the scorecard metrics that you want to see on the OT Progress Scorecard. You can filter by one or more business units, their respective sites, and a specific calendar month.

Business unit filter

The business unit (BU) filter lets you do the following actions:

- View the scorecard metrics for all business units.
- View the scorecard metrics for a specific business unit.
- View the scorecard metrics for multiple business units.

By default, the scorecard shows the metrics for all of your available BUs.

After you set the BU filter, the scorecard displays the data from every site that is included in the selected BUs. You can then select a site from the All Sites menu, which is described in the next section. If you change the BU filter and select different BUs, the site filter is updated to only include the sites that are associated with the BU that you selected.

For more information about how to use BU and site filters, see Use the Operational Technology Progress Scorecard filters.

Site filter

The site filter lets you do the following actions:

- View the scorecard metrics for all sites.
- View the scorecard metrics for a specific site.
- View the scorecard metrics for multiple sites.

By default, the scorecard shows the metrics for all sites.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Date filter

The date filter lets you view the scorecard metrics for a specific calendar month in the selected year. By default, the scorecard shows the metrics for the previous month and year.

Note: If the [PA OTPSC] Monthly Data Collection job hasn't run yet, the scorecard shows a score of 0. For more information about the [PA OTPSC] Monthly Data Collection job, see Configure the data collection for the Operational Technology Progress Scorecard.

Use the Operational Technology Progress Scorecard filters

Use the business unit (BU) and site filters on the Operational Technology (OT) Progress Scorecard to filter the data by business unit, site, or date.

Before you begin

Role required: admin

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Open the OT Progress Scorecard.
3. View the scorecard metrics for one or more BUs.
   a. In the header, select the **All business units** menu.
   b. From the list, select one or more BUs that you want to see the data for. You can use the search function to search for a specific BU.
4. View the scorecard metrics for one or more sites.
   a. In the header, select the **All sites** menu.
   b. From the list, select one or more sites that you want to see the data for.

      Note: You can use the search function to search for a specific site. Enter the name of the site or the short code in the search bar. The short code is an abbreviation for your site.

5. View the scorecard metrics for a calendar date.
   a. In the header, select the calendar ( ) icon.
   b. Select the month and year that you want to the data for.

Sort the Operational Technology Progress Scorecard by ascending or descending order

Sort the Operational Technology (OT) Progress Scorecard by ascending or descending order to customize your view of the scorecard.

Before you begin

Role required: ot_progress_scorecard_viewer

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. Select the **OT Progress Scorecard** ( ) icon.
3. Select the Ascending ( ) or Descending ( ) icon.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Result
The OT Progress Scorecard is now organized by ascending or descending order. If you log out, the sort configuration is saved for the next time you log in.

Configure the order of your important actions on the Operational Technology Action-Oriented Landing Page

Configure the order of your important actions on the Operational Technology (OT) Action-Oriented Landing Page to personalize how you view your tasks.

Before you begin
Role required: cmdb_ot_viewer

Procedure
1. Navigate to **All** > **Industrial Workspace**.
2. To the **Home** () icon.
3. Select the **Configure important actions** () icon.
4. Select **Sort items**.
5. In the **Select attribute** field, select the attribute that you want your important actions to be filtered by.
   You can use the **Search** field to find the attribute you want to sort your actions by.
6. In the **Order** field, select **Ascending** or **Descending**.

Operational Technology Vulnerability Risk Rollup dashboard

The Operational Technology (OT) Vulnerability Risk Rollup dashboard contains the risk score of the OT devices at each level of the equipment model.

OT Vulnerability Risk Rollup dashboard overview

The OT Vulnerability Risk Rollup dashboard contains two tables for your vulnerability risk scores.

- Vulnerability risk table for your equipment model entities
- Vulnerability risk table for OT devices with no site assigned

OT Vulnerability Risk Rollup dashboard tables

Table	Description
Vulnerability risk table for your equipment model entities	Table that displays the risk scores for your site's equipment model entities and their vulnerable items. It also highlights the area that poses the most risk and the number of vulnerable items.
Vulnerability risk table for no site assigned OT devices	Table that displays the risk scores and count of vulnerable items for OT devices that are not assigned to any site

Required roles to view the dashboard

To access the OT Vulnerability Risk Rollup dashboard, you must have the **sn_otvr.remediation_owner** role.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Site filter

You can use the **Site** filter to search for and select the site that you want to view on the dashboard. To access and use the site filter, you must have the **cmdb_ot_isa_viewer** role with access to the site you want to view.

For more information, see Use the site filter.

Indicator sources and indicators for the Operational Technology Vulnerability Response (PA) dashboard

The Operational Technology Vulnerability Response application uses indicator sources and indicators to gather data and track the progress of your vulnerability remediation.

Indicator sources

The Operational Technology Vulnerability Response indicators gather data from the following indicator sources. If you expect more than 1 million records to be collected from the indicator sources, you must override the expected count in the Records collection section of the indicator source. For more information, see Review the indicator sources for a larger number of records.

OTVI.New

Uses the sn_vul_vulnerable_item table and collects the new OT vulnerable items.

OTVI.Active

Uses the sn_vul_vulnerable_item table and includes all the active vulnerable items in your OT system.

OTVI.Closed

Uses the sn_vul_vulnerable_item table and includes all the closed vulnerable items in your OT system.

OTRT.Active

Uses the sn_vul_vulnerablity table and includes all the active remediation tasks in your OT system.

Indicators

Several indicators are used to measure and track the progress of your vulnerability remediation in the Operational Technology Vulnerability Response application.

The **collect records** option for the indicators is inactive by default for the Operational Technology Vulnerability Response application. This option is turned off to avoid the performance issues that may occur when you collect a large amount of data for each indicator.

OT Vulnerable Items

Number of the OT vulnerable items on the data source OTVI.Active, which uses the sn_vul_vulnerable_item table. The goal is to minimize the number of vulnerable items in your system.

OT Critical Vulnerable Items

Number of the OT critical vulnerable items on the data source OTVI.Active, which uses the sn_vul_vulnerable_item table. The goal is to minimize the number of critical vulnerable items in your system.

OT Unassigned Vulnerable Items

All active OT Vulnerable Items where both the Assignment Group and Assigned To fields are empty. The goal is to minimize the number of unassigned vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Closed Vulnerable Items

The OT Closed Vulnerable Items indicator is measured daily as a unit number. The goal is to maximize the number of closed vulnerable items in your system.

OT Deferred Vulnerable Items

Number of OT deferred vulnerable items on the data source OTVI.Active, which uses the sn_vul_vulnerable_item table. The goal is to minimize the number of deferred vulnerable items in your system.

OT Critical Deferred Vulnerable Items

Number of OT critical deferred vulnerable items on data source OTVI.Active, which uses the sn_vul_vulnerable_item table. The goal is to minimize the number of critical deferred vulnerable items.

OT Non-Deferred Overdue Critical Vulnerable Items

Number of OT non-deferred overdue critical vulnerable items on the data source OTVI.Active, which uses the sn_vul_vulnerable_item table. The goal is to minimize the number of non-deferred overdue critical vulnerable items in your system.

OT Remediation Tasks

Number of OT remediation tasks on the data source OTRT.Active, which uses the sn_vul_vulnerability table. The goal is to minimize the number of remediation tasks in your system.

OT Non-Deferred Overdue Critical Remediation Tasks

Number of OT non-deferred overdue critical remediation tasks on the data source OTRT.Active, which uses the sn_vul_vulnerability table. The goal is to minimize the number of non-deferred overdue critical remediation tasks in your system.

OT Non-Deferred Remediation Tasks

Number of OT non-deferred remediation tasks on the data source OTRT.Active, which uses the sn_vul_vulnerability table. The goal is to minimize the number of non-deferred remediation tasks in your system.

OT Non-Deferred Critical Remediation Tasks

Number of OT non-deferred critical remediation tasks on the data source OTRT.Active, which uses the sn_vul_vulnerability table. The goal is to minimize the number of non-deferred critical remediation tasks in your system.

OT Unassigned Remediation Tasks

All active remediation tasks where both the Assignment Group and Assigned To fields are empty. The goal is to minimize the number of unassigned remediation tasks in your system.

% Vulnerable Items Met Remediation Target

```
([[Closed Vulnerable Items > Remediation Target = Target
Met]] / [[Closed Vulnerable Items]]) * 100
```

The goal is to maximize the percentage of vulnerable items that meet the remediation target in your system.

OT Vulnerable Item Mean Time to Remediate

```
[[Summed Duration of Closed Vulnerable Items]] / [[Closed
Vulnerable Items]]
```

OT Summed Duration of Closed Vulnerable Items

Number of OT summed duration of closed vulnerable items on the data source OTVI.Closed, which uses the sn_vul_vulnerable_item table. The goal is to minimize the summed duration of the closed vulnerable items in your system.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Operational Technology Vulnerability Response (PA) dashboard breakdowns

The Operational Technology Vulnerability Response uses breakdowns to filter and group the collected records.

The following breakdowns apply to the indicators on the dashboard.

Age

Age of the vulnerable item that is displayed in the Days/Hours/Minutes format.

Age Closed

Age of the vulnerable item when its state changes to Closed.

Assignment Group

Assignment group of the vulnerable item or remediation task.

CI Manager

Manager of vulnerable configuration items (CIs).

Deferral Reason

Reason that a vulnerable item is deferred for remediation.

Exploit Attack Vector

Most vulnerable attack vector of the exploits for a vulnerability.

Exploit Exists

Exploit that is associated with a vulnerability.

Exploit Skill Level

Lowest skill level required to exploit a vulnerability.

Remediation Target Rule

Expected time frame for remediating a vulnerable item.

Remediation Target Status

Updated status of a vulnerable item with a remediation target date.

Remediation Target Status (Closed)

Updated status of a vulnerable item when the remediation target date is met.

Risk Rating

Quantified Risk Score that separates the vulnerable items into Critical, High, Medium, Low, and None.

Severity

Normalized degree of severity of a vulnerability.

State

State of a vulnerable item or remediation task.

The following breakdown sources apply to the indicators on the dashboard for vulnerable item reports, remediation task reports, or both types of reports.

Assignment Group

Vulnerable item and remediation task reports.

Deferred.Reason.Non.Closed

Vulnerable item reports.

Exploit Attack Vector

Vulnerable item reports.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exploit Exists

Vulnerable item reports.

Exploit Skill Level

Vulnerable item reports.

OT Age Range

Vulnerable item reports.

Remediation Target Status

Vulnerable item and remediation task reports.

Remediation Target Status (Closed)

Vulnerable item and remediation task reports.

Remediation.Target.Rule

Vulnerable item and remediation task reports.

Risk Rating

Vulnerable item and remediation task reports.

Severity

vulnerable item and remediation task reports.

State

Vulnerable item and remediation task reports.

Vulnerable.Item.CI.Manager

Vulnerable item reports.

Operational Technology Vulnerability Response (PA) dashboard collection jobs

The Operational Technology Vulnerability Response (PA) dashboard uses collection jobs to collect the data that is shown on the dashboard.

The following collection jobs collect the data that is shown on the Operational Technology Vulnerability Response (PA) dashboard:

[PA OT VR] Historical Vulnerability Data Collection

Collection job for the historical data of existing records.

> **Note:** The Historical Vulnerability Data Collection is an on-demand job that you only need to execute once. After the historical data is collected, the daily data collection jobs run on a scheduled time every day. For more information, see Collect historical data.

[PA OT VR] Daily Collection for Remediation Tasks

Collection job for the remediation task data that occurs daily.

[PA OT VR] Daily Collection for Vulnerable Items 1

Collection job that occurs daily for non-deferred overdue critical vulnerable items, deferred vulnerable items, vulnerable items, and critical vulnerable items.

[PA OT VR] Daily Collection for Vulnerable Items 2

Collection job that occurs daily for unassigned vulnerable items, closed vulnerable items, summed duration of closed vulnerable items, and critical deferred vulnerable items.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Data visualizations used in the Operational Technology Vulnerability Response (PA) dashboard

The Operational Technology Vulnerability Response (PA) dashboard uses data visualizations to display your OT vulnerability data.

The following tables describe the data visualizations shown in the Operational Technology Vulnerability Response (PA) dashboard.

Vulnerable Items tab data visualizations

Name	Type	Description
Total OT Vulnerable Items	Bar	Bar chart that displays the active (non-closed) OT vulnerable items grouped by device type.
New OT Vulnerable Items	Pie	Pie chart that displays the new OT vulnerable items that were found in your system grouped by device type.
OT Unassigned Vulnerable Items	Pie	Pie chart that displays the OT vulnerable items grouped by device type that are open and haven't been assigned to a user.
OT Vulnerable Items by State	Bar	Bar chart that displays all the vulnerable items by state. You can interpret how many vulnerabilities are being addressed and how many need further investigation. For example, if the **Under Investigation** category is relatively high, you can prioritize these items by addressing those vulnerable items first.
OT Vulnerable Items by Risk Rating	Bar	Number of the active OT vulnerable items that are grouped by the risk rating over the selected time span.
OT VIs Met Remediation Target	Singe score	Percentage of the closed OT vulnerable items that have met their remediation target dates in the current and previous quarters. Remediation targets are calculated from the Last Opened date plus the number of days since the Last Opened date (measured as 24-hour increments).

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Vulnerable Items tab data visualizations (continued)

Name	Type	Description
OT VI Mean Time to Remediate (MTTR)	Single score	Mean time to remediate (close) an OT vulnerable item, displayed as a 30-day running average. **Note:** The value for Age Closed is calculated when the data is collected. The value is the difference between the last_opened date and the date and time of the collection job.
OT VI by age	Bar	Bar chart that displays the OT active vulnerable items grouped by age (in days).
OT Closed Vulnerable Items by Remediation Target Status	Bar	Number of the closed OT vulnerable items that are grouped by the remediation target status over the selected time span. **Note:** The value for Age Closed is calculated when the data is collected. The value is the difference between the last_opened date and the date and time of the collection job.
OT Critical Vulnerable Item by Assignment Group	Indicator scorecard	Critical VIs organized by assignment group.
OT Overdue Critical Vulnerable Items by Assignment Group	Indicator scorecard	Critical VIs that are overdue organized by assignment group.

Remediation tab data visualizations

Name	Type	Description
OT Remediation Tasks	Single score	Number of the active (non-closed) OT remediation tasks.
OT Critical Remediation Tasks Near Due	Single score	Number of the active OT remediation tasks that are approaching their remediation target date.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Remediation tab data visualizations (continued)

Name	Type	Description
		The remediation target date of an OT remediation task is set to the closest due date that belongs to an active vulnerable item in the group. The remediation targets are calculated from the Last Opened date plus the number of days (measured as 24-hour increments). This report excludes the deferred OT remediation tasks.
OT Remediation Task by Risk rating	Bar	Bar chart that displays the active OT remediation tasks grouped by the risk rating.
OT Remediation Task by Target Status	Bar	Bar chart that displays the active OT remediation tasks grouped by the remediation target status. This report excludes the deferred OT vulnerable items.
OT Remediation Task by State	Bar	Bar chart that displays all the remediation tasks by state. You can interpret the progress of your remediation tasks.
OT Unassigned Remediation Tasks	Single score	Number of the active OT remediation tasks without an assignee or assignment group.
OT Critical Remediation Task by Assignment Group	Indicator scorecard	Critical remediation tasks organized by assignment group.
OT Overdue Critical Remediation Task by Assignment Group	Indicator scorecard	Critical remediation tasks that are overdue organized by assignment group.

Exception tab data visualizations

Name	Type	Description
OT Deferred Vulnerable Items by Reason	Bar	Number of the deferred OT vulnerable items that are grouped by the deferral reason.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Exception tab data visualizations (continued)

Name	Type	Description
OT Exceptions for Critical Vulnerable Items by Assignment Group	Indicator scorecard	Exceptions for critical VIs organized by assignment group.

View an Operational Technology Unified Map

View an Operational Technology (OT) Unified Map in the Industrial Workspace that displays the relationships between devices and other CIs.

Before you begin

Role required: admin

About this task

You can access the OT Unified Map in the following locations in the Industrial Workspace.

- ISA record in the Equipment Model Manager
- OT incident record
- OT change record

Procedure

1. Navigate to **All** > **Industrial Workspace**.
2. To access the OT Unified Map in an equipment model entity record, complete the following actions.
   a. Open the Equipment Model Manager by selecting the Equipment Model ( ) icon.
   b. Open the equipment model entity record that you want to view the Unified Map for.
   c. Select the **View OT Unified Map** button.
3. To access the OT Unified Map in a related record, such as an OT incident record, or change record, complete the following actions.
   a. Open the Industrial Workspace list view by selecting the List ( ) icon.
   b. Select the record that you want to view the Unified Map for.

      For example, if you want to view the Unified Map for an OT incident record, select one of the available lists under the **OT Incidents** module and open the record.
   c. To open the map in a new window, select the **View OT Unified Map** button.
   d. To open the map in the side panel of the record, select the **OT Health** ( ) icon.

What to do next

You can now view the OT Unified Map. On the Unified Map, you can also see the highlighted nodes of the following related items.

- Past OT Changes
- Current OT Changes
- Planned OT Changes

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Active OT Incidents
- Active OT Alerts
- OT Vulnerable Items

View a daily summary of Operational Technology device activities for an Equipment Model Entity

In the Equipment Model View of the Industrial Workspace, view the previous day's actions and changes that have been performed on the Operational Technology (OT) devices in a site.

Before you begin

Role required: cmdb_ot_isa_viewer

About this task

In the Equipment Model menu of the Industrial Workspace, the **Daily Activity** tab displays the number of activities that were performed on the OT devices in your site for the previous day. The **Daily Activity** tab displays the following activities:

- An OT device has been added to the site.
- An OT device details have been updated.
- An OT device has been mapped to a new equipment model entity.
- An OT device lifecycle status has been marked as retired.

Procedure

1. Navigate to **All** > **Industrial Workspace** > **Equipment Model menu (**  **) icon.**.
2. Select the equipment model entity record for which you want to view the Daily Summary of its OT devices.

What to do next

You can view the total number of activities in the **Daily Activity** tab. If you want to view an expanded list of all the activities that have been performed on the OT devices on the previous day, select the **Daily Activity** tab. In the expanded list, you can view the activity details such as:

- OT device type
- Mapped equipment model entity
- Change status
- Device criticality
- Discovery Source
- Changed by
- Changed field
- Field changes

Note: The daily activity records, which are older than two days are automatically deleted.

Use the Hardware Vulnerability Assessment menu in the Industrial Workspace

Use the *Hardware Vulnerability Assessment* menu to view and track all the firmware vulnerability assessments in your OT environment. Also, in the HVA menu you can view the vulnerable items that are created based on the firmware vulnerability assessments.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before you begin
Role required: sn_otvr.vul_event_manager

About this task
The *Hardware Vulnerability Assessment* menu provides information of all vulnerabilities in the Operational Technology (OT) inventory that match fully or partially to the vulnerabilities enlisted in the National Vulnerability Database (NVD).

Procedure
1. Navigate to **Workspaces** > *Industrial Workspace* > *Hardware Vulnerability Assessment*. **Select the menu icon ( )**.
2. Perform the following actions on the **Fully matched assessments**, **Partially matched assessments**, **Vulnerable Items**, **Ignored assessments**, and **Awaiting Normalization** tabs as needed:
   a. Select More Actions icon ( ) and then select **Personalized fields**. Choose additional columns and view them for more information regarding the assessment.
   b. Update the displayed list of assessments by selecting the refresh icon ( ).
   c. View assessment information in the tab according to the additional filter conditions that you select from the filter list icon ( ) icon.
   d. Perform a quick filtration of assessments by selecting **Choose Filters**.
3. View the assessment records by selecting the **Fully matched assessments** and **Partially matched assessments** tabs.
   a. You can manually create vulnerable items for any assessment records that you choose. Select one or more records from the displayed list and then select **Create Vulnerable Items**.
   b. You can ignore assessment records that you choose from the displayed list. Select one or more assessment records and then select **Ignore**. These ignored assessments are available on the **Ignored assessments** tab.
4. On the **Ignored assessments** tab:
   a. If you want to perform assessments on the OT devices that you have ignored previously, select **Revert**.
   b. If you want to create vulnerable items manually for the assessments that you choose from the displayed list, select **Create Vulnerable Items**.
5. The **Vulnerable Items** tab View the list of vulnerability items that are created based on the assessment records created in the **Fully matched assessments**, **Partially matched assessments**, and **Ignored assessments** tabs.
6. View the OT device data that hasn't been used for assessment and awaiting normalization, by selecting the **Awaiting Normalization** tab.
   The device data may have the following normalization status:
   - **New**
   - **Match not found**
   - **Publisher normalized**

Important: Enable the Opt-in feature in Enterprise Asset Management, which enables OT devices to be available for normalization. For more information, see Opt-in to the Enterprise Asset Management Content Service.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Operational Technology Hardware Vulnerability Assessment

Set up the Hardware Vulnerability Assessment of Operational Technology devices using guided setup

View and edit the OT Network Map

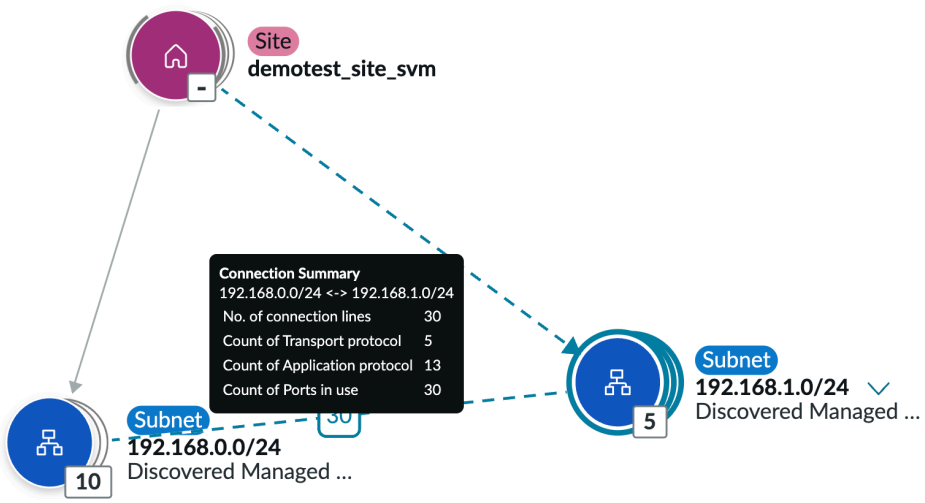
View and edit the Operational Technology (OT) Network Map in the Industrial Workspace to visualize your OT networks per site and their OT devices.

Before you begin

Role required: cmdb_ot_isa_viewer role and cmdb_ot_viewer

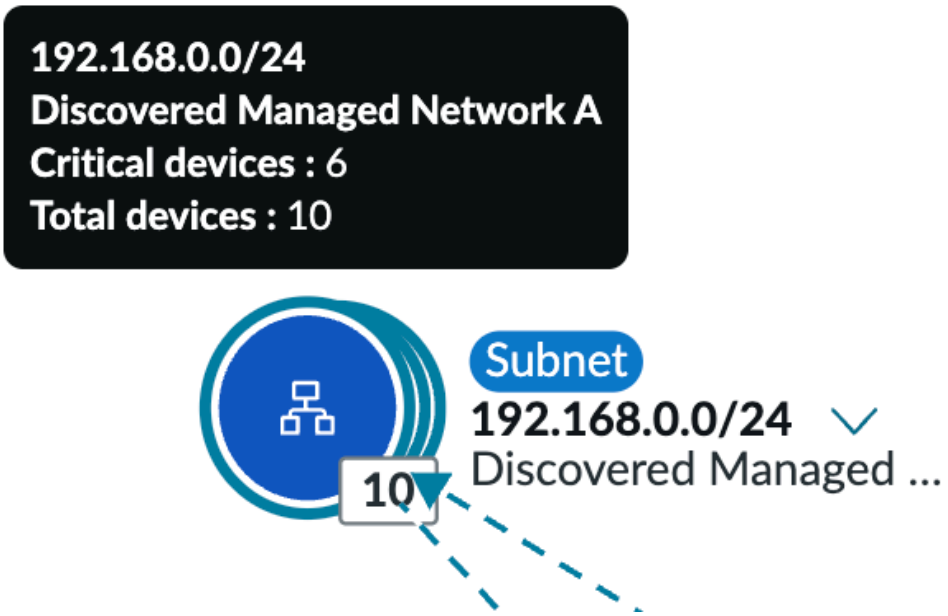
Procedure

1. Navigate to the Industrial Workspace.
2. To open the Equipment Model Manager, select the **Equipment model** icon.
3. Select a site that you want to view the OT Network Map for.
4. Select **View OT Network Map**.
   The network map opens in a new tab.
5. To view the legend with an explanation of the visuals used in the network map, select the **Legend** icon.
6. To view additional information about a subnet node, hover your mouse over the node.
7. To view additional information about a device node, hover your mouse over the node.
8. To view the **Connection Summary** between subnet nodes, hover over the dashed line between the nodes as shown in the following image.



9. To expand a subnet and view its individual device nodes, select the number on the subnet node.
   The number on the subnet node represents the total number of devices in the subnet. The following image shows an example of the device number.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

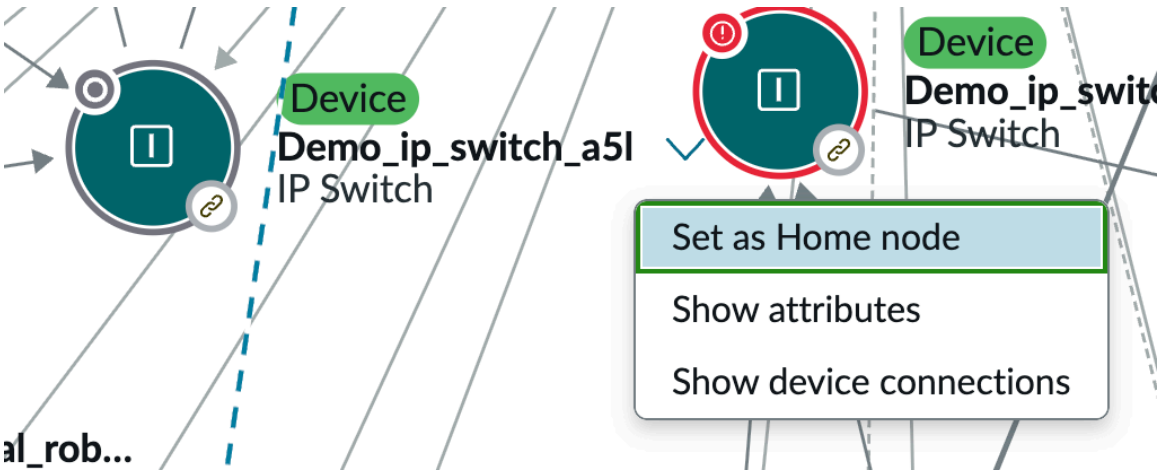


Note: You can only expand one subnet at a time. For example, if Subnet A is expanded and you try to expand Subnet B, Subnet A automatically collapses.

10. To set a device node as the home node, complete the following steps.

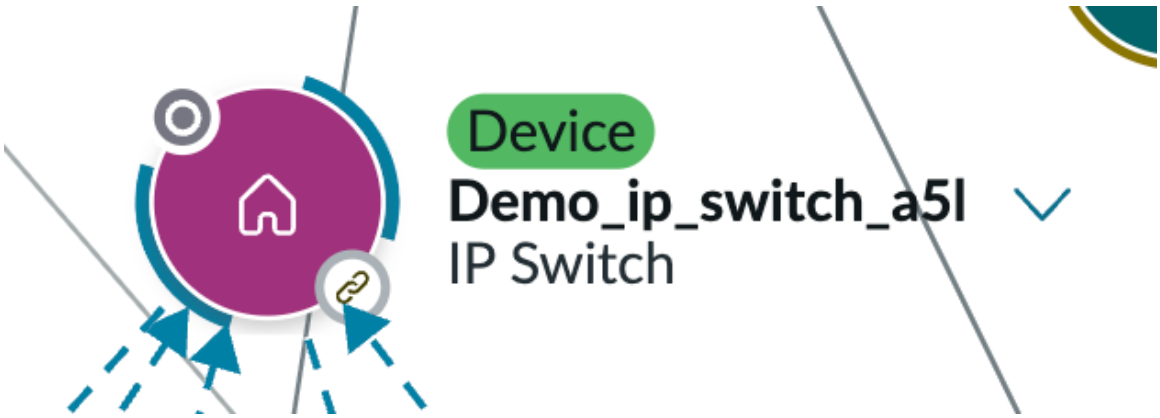
a. To access the contextual actions, right-click the node or next to the device node name, select the dropdown.

b. Select **Set as Home node**.

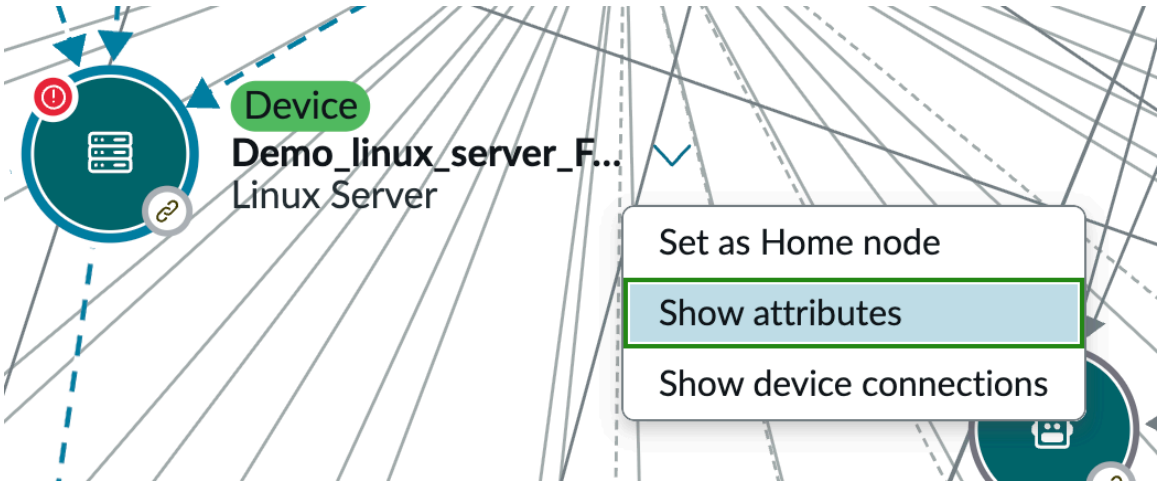


© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The selected device node is set as the home node and the node icon changes as shown in the following image.



11. To view the attributes for a device node, complete the following steps.
    a. To access the contextual actions, right-click the node or next to the device node name, select the dropdown.
    b. Select **Show attributes**.

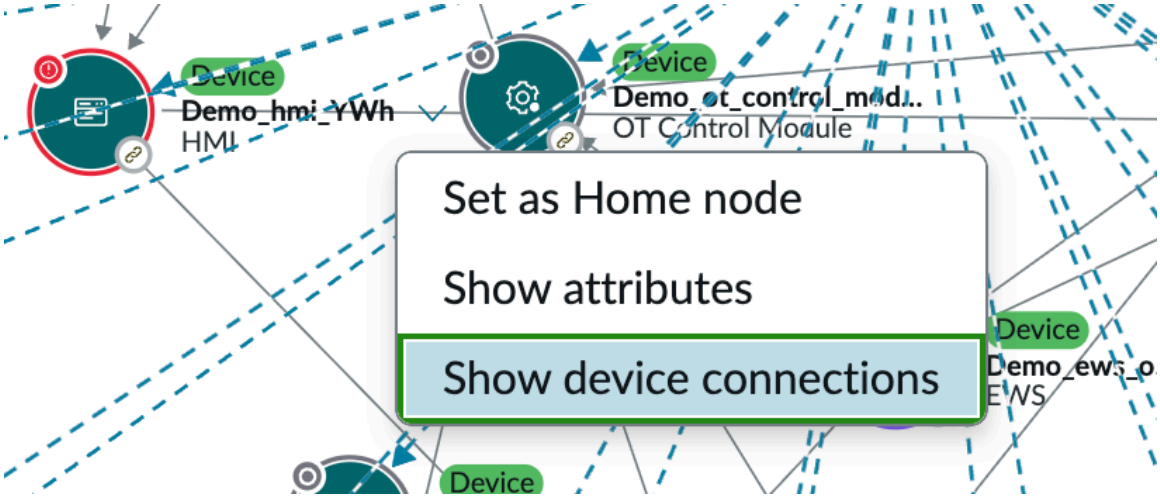


A side panel opens that shows the following attributes for the selected device node:

- Class
- Updated
- Location
- Owned by
- Most recent discovery
- Discovery source

12. To view the device connections for a device node, complete the following steps.
    a. To access the contextual actions, right-click the node or next to the device node name, select the dropdown.
    b. Select **Show device connections**.

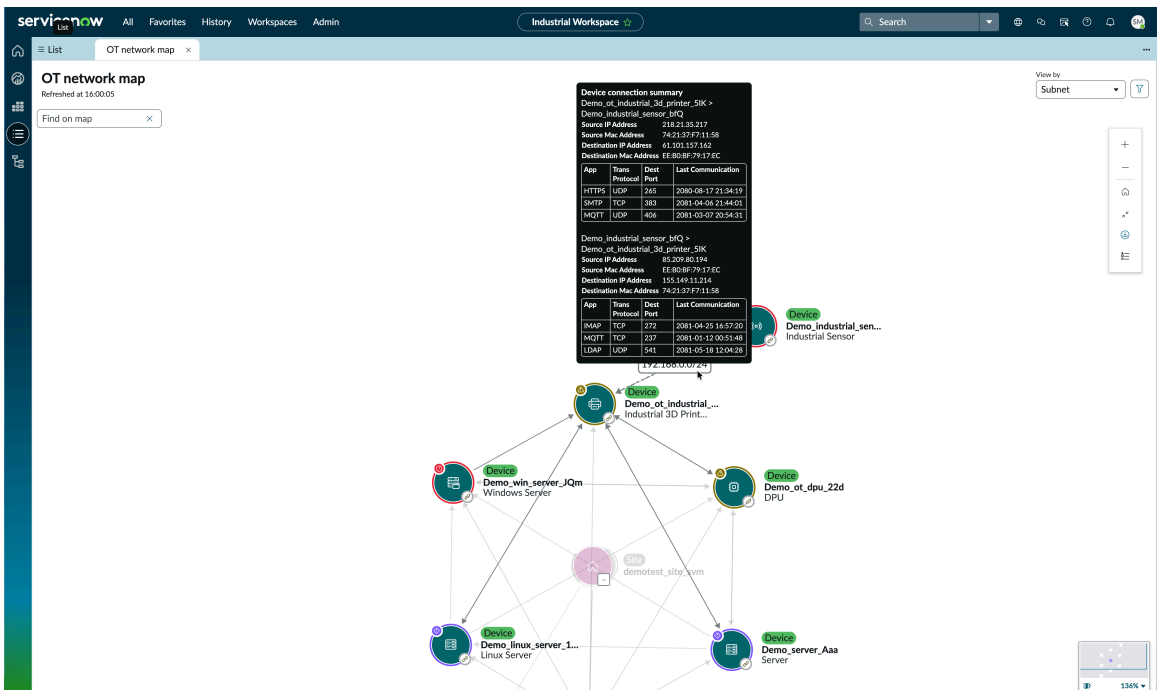
© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



The network map updates to highlight the device-to-device connections and to show both connections within the same subnet, represented by a solid line, and cross-subnet connections, represented by a dashed line.

c. To see the **Device connection summary** details, hover over the IP address on the dashed line or hover over the solid line.

The following image shows an example of the device connection summary on the dashed line.



d. To escape this view, select the dropdown again and click **Hide device connections**.

13. To apply filters to the map to refine the nodes shown, complete the following steps.

a. Select the **Filters** Filter icon.

b. Select or deselect the options available under the following filter categories.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

OT Network Map filters

Filter	Description
Class	The name of the assigned class for the OT device.
Criticality	The measure of the relative risk to the site process due to failure of the device.
Manufacturer	The device manufacturer.
Purdue level	The assigned Purdue level. Ranges 0–5.
Discovery source	The Discovery source for the OT device data.

c. Select **Apply**.

d. To return to the default settings, select **Reset filters** and click **Apply**.

14. To search for a subnet, device node, managed network, and so on in the node map, use the **Find on map** search bar.

15. To align the map back on the home node, select the **Align to home node** icon in the control panel.

Domain separation and Operational Technology

Domain separation is supported for Operational Technology. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

Operational Technology domain separation overview

Because each application can have its own domain separation relationship, no single support level applies to Operational Technology. For more information, see Domain separation and Workflow Studio.

The following table describes the domain separation support levels and use cases for each Operational Technology application.

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Support levels by application

Application	Support level
Operational Technology Manager	Basic
Industrial Process Manager	Basic
Operational Technology Vulnerability Response	Basic
Operational Technology	Basic
Operational Technology Change Management	Basic
Operational Technology Knowledge Management	Basic
Operational Technology Request Management	Basic

Related topics

Domain separation for service providers

© 2026 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.